PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-298449
(43)Date of publication of application : 26.10.2001

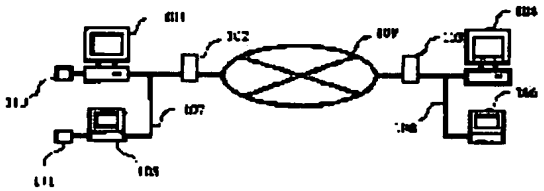
(51)Int.Cl. H04L 9/14
G06F 15/00

(21)Application number : 2000-110651
(22)Date of filing : 12.04.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : YAMAGUCHI MASAFUMI
TANAKA YUTAKA
YAMAUCHI HIROTAKA
OTA YUSAKU

(54) SECURITY COMMUNICATION METHOD, COMMUNICATION SYSTEM AND ITS UNIT

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a security communication unit, system and method that can set a level of security communication by each user for data transmission, easily revise a connection parameter of various security communications and automatically set a level of the security communication with a connection destination.
SOLUTION: Cross-reference information cross-referencing information of a user, using a communication terminal with a security type, is stored, and the security type is decided from the cross-reference information. Furthermore, cross-reference information cross-referencing Internet address information with the security type is stored, and the security type is decided from the cross- reference information on the basis of the Internet address information. Furthermore, the security type is inquired of a prescribed security information unit, and the security type is decided on the basis of a reply of the inquiry.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－298449
（P2001－298449A）
(43)公開日　平成13年10月26日(2001.10.26)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　9/14		Ｇ０６Ｆ　15/00	３３０Ａ	５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０	Ｈ０４Ｌ　9/00	６４１	５Ｊ１０４

審査請求　未請求　請求項の数40　ＯＬ　（全 21 頁）

(21)出願番号　特願2000－110651(P2000－110651)

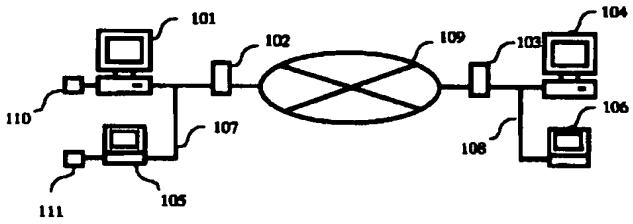
(22)出願日　平成12年４月12日(2000.4.12)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　山口　雅史
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　田中　豊
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100083172
弁理士　福井　豊明

最終頁に続く

(54)【発明の名称】　セキュリティ通信方法、通信システム及びその装置

(57)【要約】
【課題】　データ送信を行うユーザごとにセキュリティ通信のレベルを設定でき、容易に各種セキュリティ通信の接続パラメータを変更でき、接続先とのセキュリティ通信のレベルを自動で設定するセキュリティ通信装置、システム、及び方法を提供する。
【解決手段】通信端末を使用するユーザの情報とセキュリティ種を対応付けた対応情報を記憶し、上記対応情報からセキュリティ種を決定する。又、インターネットアドレス情報と、セキュリティ種とを対応付けた対応情報を記憶し、上記インターネットアドレス情報に基づいて、上記対応情報からセキュリティ種を決定する。さらに、セキュリティ種を所定のセキュリティ情報装置に問い合わせ、該問い合わせの回答に基づいて上記セキュリティ種を決定する。



1

【特許請求の範囲】

【請求項１】　送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキュリティを確保するセキュリティ通信装置において、
上記送信元通信端末を使用するユーザの情報とセキュリティ種を対応付けた対応情報を記憶する記憶手段と、
上記ユーザの情報に基づいて、上記対応情報からセキュリティ種を決定するセキュリティ種選択手段を備えることを特徴とするセキュリティ通信装置。

【請求項２】　上記セキュリティ種選択手段が、さらに上記対応情報の変更時に、上記変更後の情報に基づいた通信の確立を直ちに確認する請求項１に記載のセキュリティ通信装置。

【請求項３】　上記セキュリティ種選択手段が決定するセキュリティ種が、セキュリティプロトコルの種類である請求項１又は２に記載のセキュリティ通信装置。

【請求項４】　上記セキュリティプロトコルが、ＩＰＳＥＣである請求項３に記載のセキュリティ通信装置。

【請求項５】　上記セキュリティ種選択手段が決定するセキュリティ種が、セキュリティ通信時に使用する定義情報群である請求項１又は２に記載のセキュリティ通信装置。

【請求項６】　上記定義情報群が、セキュリティポリシーである請求項５に記載のセキュリティ通信装置。

【請求項７】　上記定義情報群が、認証アルゴリズム又は暗号化アルゴリズムの少なくとも１つを含む請求項５に記載のセキュリティ通信装置。

【請求項８】　送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキュリティを確保するセキュリティ通信システムにおいて、
上記送信元通信端末を使用するユーザの認証を行うユーザ認証手段と、
上記ユーザとセキュリティ種を対応付けた対応情報を記憶する記憶手段と、
上記ユーザ認証手段により認証されたユーザの情報に基づいて、上記対応情報からセキュリティ種を決定するセキュリティ種選択手段を備えることを特徴とするセキュリティ通信システム。

【請求項９】　上記セキュリティ種選択手段が、さらに上記対応情報の変更時に、上記変更後の情報に基づいた通信の確立を直ちに確認する請求項８に記載のセキュリティ通信システム。

【請求項１０】　ネットワークを介して接続される通信端末間の、通信のセキュリティを確保するセキュリティ通信方法において、
上記通信端末を使用するユーザの情報に基づいてセキュリティ種を決定することを特徴とするセキュリティ通信方法。

【請求項１１】　送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキュリティを確保するセキュリティ通信装置において、

2

上記送信元通信端末にて動作するアプリケーションに入力されるインターネットアドレス情報と、セキュリティ種とを対応付けた対応情報を記憶する記憶手段と、
上記インターネットアドレス情報に基づいて、上記対応情報からセキュリティ種を決定するセキュリティ種選択手段を備えることを特徴とするセキュリティ通信装置。

【請求項１２】　上記対応情報が、さらに上記送信元通信端末を使用するユーザの情報とセキュリティ種とが対応付けられているとともに、
上記ユーザの情報にも基づいて上記セキュリティ種を決定する請求項１１に記載のセキュリティ通信装置。

【請求項１３】　上記セキュリティ種の決定を、視覚化された上記セキュリティ種の一覧に対して同様に視覚化された上記インターネットアドレス情報を視覚的に対応付けることにより行う請求項１１又は１２に記載のセキュリティ通信装置。

【請求項１４】　上記インターネットアドレス情報のＩＰアドレスへの変換に、ドメインネームシステムサーバを利用する請求項１１に記載のセキュリティ通信装置。

【請求項１５】　上記セキュリティ種が、セキュリティプロトコルである請求項１１～１４のいずれか１項に記載のセキュリティ通信装置。

【請求項１６】　上記セキュリティプロトコルが、ＩＰＳＥＣである請求項１５に記載のセキュリティ通信装置。

【請求項１７】　上記セキュリティ種が、セキュリティ通信時に使用する定義情報群である請求項１１～１４のいずれか１項に記載のセキュリティ通信装置。

【請求項１８】　上記定義情報群が、セキュリティポリシーである請求項１７に記載のセキュリティ通信装置。

【請求項１９】　上記定義情報群が、認証アルゴリズム又は暗号化アルゴリズムの少なくとも１つを含む請求項１７に記載のセキュリティ通信装置。

【請求項２０】　送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキュリティを確保するセキュリティ通信システムにおいて、
上記送信元通信端末にて動作するアプリケーションに入力されるインターネットアドレス情報と、セキュリティ種とを対応付けた対応情報を記憶する記憶手段と、
上記インターネットアドレス情報に基づいて、上記対応情報からセキュリティ種を決定するセキュリティ種選択手段を備えることを特徴とするセキュリティ通信システム。

【請求項２１】　さらに上記送信元通信端末を使用するユーザの認証を行うユーザ認証手段を備えるとともに、
上記対応情報が、上記送信元通信端末を使用するユーザの情報とセキュリティ種とが対応付けられ、
上記ユーザの情報にも基づいて上記セキュリティ種を決

定する請求項２０に記載のセキュリティ通信システム。

【請求項２２】　上記セキュリティ種の決定を、視覚化された上記セキュリティ種の一覧に対して同様に視覚化された上記インターネットアドレス情報を視覚的に対応付けることにより行う請求項２０又は２１に記載のセキュリティ通信システム。

【請求項２３】　ネットワークを介して接続される通信端末間の、通信のセキュリティを確保するセキュリティ通信方法において、

上記通信端末にて動作するアプリケーションに入力されるインターネットアドレス情報と、セキュリティ種とを対応付け、

上記インターネットアドレス情報に基づいてセキュリティ種を決定することを特徴とするセキュリティ通信方法。

【請求項２４】　通信端末を特定する端末特定情報と、該通信端末との通信において推奨されるセキュリティ種とを対応付けた対応情報を記憶する記憶手段と、

上記通信端末とは異なる端末からの、上記通信端末について推奨されるセキュリティ種の問い合わせに対し、上記端末特定情報に基づいて、上記対応情報から上記推奨されるセキュリティ種を選択する推奨セキュリティ種管理手段と、

上記選択された推奨されるセキュリティ種を送信する送信手段を備えることを特徴とするセキュリティ情報装置。

【請求項２５】　さらに、上記端末特定情報が上記対応情報に無い場合に、上記通信端末に対して、該通信端末との通信において推奨されるセキュリティ種を問い合わせる問い合わせ手段を備える請求項２４に記載のセキュリティ情報装置。

【請求項２６】　上記セキュリティ種が、セキュリティプロトコルである請求項２４又は２５に記載のセキュリティ情報装置。

【請求項２７】　上記セキュリティプロトコルが、ＩＰＳＥＣである請求項２６に記載のセキュリティ情報装置。

【請求項２８】　上記セキュリティ種が、セキュリティ通信時に使用する定義情報群である請求項２４又は２５に記載のセキュリティ情報装置。

【請求項２９】　上記定義情報群が、セキュリティポリシーである請求項２８に記載のセキュリティ情報装置。

【請求項３０】　上記定義情報群が、認証アルゴリズム又は暗号化アルゴリズムの少なくとも１つを含む請求項２８に記載のセキュリティ情報装置。

【請求項３１】　送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキュリティを確保するセキュリティ通信装置において、

上記セキュリティの確保に用いるセキュリティ種を所定のセキュリティ情報装置に問い合わせる問い合わせ手段と、

上記問い合わせに対応する上記所定のセキュリティ情報装置からの回答に基づいて上記セキュリティ種を決定するセキュリティ種選択手段を備えることを特徴とするセキュリティ通信装置。

【請求項３２】　上記回答が、１又は複数の上記セキュリティ種を含む請求項３１に記載のセキュリティ通信装置。

【請求項３３】　上記セキュリティ種が、セキュリティプロトコルである請求項３１又は３２に記載のセキュリティ通信装置。

【請求項３４】　上記セキュリティプロトコルが、ＩＰＳＥＣである請求項３３に記載のセキュリティ通信装置。

【請求項３５】　上記セキュリティ種が、セキュリティ通信時に使用する定義情報群である請求項３１又は３２に記載のセキュリティ通信装置。

【請求項３６】　上記定義情報群が、セキュリティポリシーである請求項３５に記載のセキュリティ通信装置。

【請求項３７】　上記定義情報群が、認証アルゴリズム又は暗号化アルゴリズムの少なくとも１つを含む請求項３５に記載のセキュリティ通信装置。

【請求項３８】　送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキュリティを確保する通信装置を備えるセキュリティ通信システムにおいて、

上記通信装置が、上記セキュリティの確保に用いるセキュリティ種を所定のセキュリティ情報装置に問い合わせる問い合わせ手段と、

上記問い合わせに対応する上記所定のセキュリティ情報装置からの回答に基づいて上記セキュリティ種を決定するセキュリティ種選択手段を備えるとともに、

上記所定のセキュリティ情報装置が、通信端末を特定する端末特定情報と、該通信端末との通信において推奨されるセキュリティ種とを対応付けた対応情報を記憶する記憶手段と、

上記通信端末とは異なる端末からの、上記通信端末について推奨されるセキュリティ種の問い合わせに対し、上記端末特定情報に基づいて、上記対応情報から上記推奨されるセキュリティ種を選択する推奨セキュリティ種管理手段と、

上記選択された推奨されるセキュリティ種を送信する送信手段を備えることを特徴とするセキュリティ通信システム。

【請求項３９】　さらに、上記所定のセキュリティ情報装置が、上記端末特定情報が上記対応情報に無い場合に、上記送信先通信端末に対して該送信先通信端末との通信において推奨されるセキュリティ種を問い合わせる問い合わせ手段を備える請求項３８に記載のセキュリティ通信システム。

5

【請求項４０】　ネットワークを介して接続される通信端末間の、通信のセキュリティを確保する通信装置を備えるセキュリティ通信方法において、
上記通信装置が、該通信装置とは異なる通信装置について推奨されるセキュリティ種を所定のセキュリティ情報装置に問い合わせ、
上記所定のセキュリティ情報装置が、上記通信装置からの上記問い合わせに対し、上記推奨されるセキュリティ種を選択して上記通信装置に送信し、
上記通信装置が上記セキュリティ情報装置から送信された上記推奨されるセキュリティ種に基づいて上記セキュリティ種を決定することを特徴とするセキュリティ通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、セキュリティ通信方法に係り、詳しくは、必要に応じてセキュリティ種を変更可能なセキュリティ通信方法、通信システム及びその装置に関するものである。

【０００２】

【従来の技術】近年、パーソナルコンピュータとインターネット技術の急激な普及により、容易でしかも安価にインターネット上に公開されるホームページによる情報提供及び情報収集が可能になっている。さらにこれだけにとどまらず、インターネットあるいは企業間のイントラネットを介した電子メールの交換や、これらを利用した電子商取引や電子決済が一般化しつつある。このようなサービスを利用する場合、特に重要な情報を含む通信には専用線並のセキュリティの確保が重要である。

【０００３】上述したようなセキュリティを確保する技術として、例えばインターネットのような広域ネットワークを仮想私設網とするＶＰＮ(Virtual Private Network)技術等のセキュリティ通信技術が注目されている。ＶＰＮを実現するセキュリティ通信のための接続手順としてトンネリングプロトコルがあり、Ｌ２Ｆ(Layer 2Forwarding)、ＰＰＴＰ(Point-to-Point Tunneling Protocol)、Ｌ２ＴＰ(Layer 2 Tunneling Protocol)、ＡＴＭＰ(Ascend Tunnel Management Protocol)、ＢａｙＤＶＳ(BayStream Dial VPN Service)、ＩＰＳＥＣ(Internet ProtocolSecurity Protocol)等が提案されている。上記セキュリティ通信のためのプロトコルを使用することにより、第３者が通信等を盗聴しうる上記広域ネットワークにおいて通信等のセキュリティを確保することが可能となる。

【０００４】これらの技術のうち、上記ＩＰＳＥＣは、ネットワーク層（ＯＳＩ参照モデル(Open System Interconnection reference model)第３層）で認証、暗号化を行うセキュリティプロトコルで、インターネット技術標準化委員会（ＩＥＴＦ）で標準化されている（ＲＦＣ２４０１から２４１２、２４５１）。上記ＩＰＳＥＣ機

6

能を搭載したコンピュータや、ネットワーク接続装置であるルータ等を介してインターネットに接続することにより、上記ＶＰＮを構築することが可能である。即ち、ユーザはネットワークの種類を意識することなく、安全にインターネットを利用することができる。尚、ＩＰＳＥＣを利用した通信を行うにあたっては、どのような認証アルゴリズムや暗号化アルゴリズムを使用するか、あるいはどのような暗号化鍵を使用するかなどを、事前に送信側と受信側のＩＰＳＥＣ機能を搭載したコンピュータまたは、ネットワーク接続装置が整合を取っておく必要がある。この認証、暗号化アルゴリズムの整合をとるための相互通信を、セキュリティ通信のための接続と呼ぶ。ＩＰＳＥＣにおいては、この接続はＳＡ（Security Association）によって実現されている。上記ＳＡは認証とセキュアメッセージ交換の機能を提供する基本的な枠組であり、通信のコンテキストを確立し、その通信のセキュリティのいくつかの側面を定義する。

【０００５】以下に、図１４、図１５、図１７、図１８を参照しながら、従来の、セキュリティ通信としてＩＰＳＥＣを用いた通信方法について説明する。又、ここに通信端末とは、ネットワーク接続装置及びコンピュータを含む。

【０００６】図１４は、従来のセキュリティ通信としてＩＰＳＥＣ機能を搭載したルータを使用してＶＰＮネットワークを構成したネットワークシステムの概略図、図１５は、上記ＩＰＳＥＣ機能を搭載したネットワーク接続装置間でのセキュリティ通信の接続手順を表した図、図１７は、従来技術におけるＩＰＳＥＣの処理方針を決めるデータベースであるＳＰＤ（Security Policy Database）の例、図１８は、従来技術におけるＳＡデータベースであるＳＡＤ（Security Association Dtabase）の例である。ここに、ＳＰＤとはセキュリティポリシーを構成するデータベースである。又、セキュリティポリシーとは、セキュリティを確保されたシステムへのアクセス規制のことであり、一般にセキュリティ要件、セキュリティ上のリスク、及びセキュリティの測定手段が含まれる。通信端末間のセキュリティを確保するシステムにおいては、セキュリティを適用する相手先通信端末を区別する情報、セキュリティを適用するかどうかの情報等を備える。尚、ＩＰＳＥＣにおいては、セキュリティポリシーは上記ＳＰＤに記述され、該ＳＰＤには送信先通信端末のＩＰアドレス、ＩＰＳＥＣ処理の有無、認証、暗号化アルゴリズム等の内容を記述した上記ＳＡが格納されるメモリ上のアドレスの位置情報を備える。

【０００７】コンピュータ１４０１はＬＡＮ１４０７(Local AreaNerwork)で他のコンピュータ１４０５及びネットワーク接続装置１４０２と接続されており、ネットワーク接続装置１４０２を経由して、外部のインターネット１４０９やイントラネット等のＷＡＮに接続されている。このインターネット１４０９には他のネットワー

ク接続装置１４０３を介してコンピュータ１４０４、１４０６が接続されるＬＡＮ１４０８が接続されている。ここで、上記ネットワーク接続装置１４０２、１４０３は、ルータ、ゲートウエイ、プロキシサーバ等のファイアウォールやＶＰＮ専用装置等である。ここで、コンピュータ１４０１他は、パーソナルコンピュータ、ワークステーション、サーバ、ノート型パソコン、ＩＰ電話、ＩＰテレビ電話、ＩＰ携帯電話等の通信機能をもつ端末であればよい。

【０００８】ここでは上記ネットワーク接続装置１４０２、１４０３にＩＰＳＥＣ機能を搭載し、ネットワーク接続装置１４０２、１４０３間でＩＰＳＥＣによる通信を行うものとして説明する。また、上記コンピュータ１４０１及び１４０４にＩＰＳＥＣ機能を搭載し、上記コンピュータ１４０１、１４０４間でＩＰＳＥＣによる通信を行うことも可能である。さらに、同様にＩＰＳＥＣ機能を搭載した、コンピュータ１４０１とＩＰＳＥＣ機能を搭載しているネットワーク接続装置１４０３間でＩＰＳＥＣによる通信を行うことも可能である。

【０００９】ところで、コンピュータ１４０１がインターネット１４０９を介してコンピュータ１４０４にデータを送信する場合には、予め上記ネットワーク接続装置１４０２、１４０３間において上記セキュリティ通信のための接続を行う必要がある。以下に該セキュリティ通信のための接続について説明する。

【００１０】ＩＰＳＥＣ通信を始めるにあたり、まず、ＩＰＳＥＣの暗号鍵交換のためのプロトコルであるＩＫＥ（Internet Key Exchange)が用いられる。該ＩＫＥを使用した通信は、ＩＫＥフェーズ１とＩＫＥフェーズ２とに分けて説明することができ、上記ネットワーク接続装置１４０２、１４０３間で行われる。尚、ＩＫＥによる自動鍵交換を行わず、手動で秘密鍵の交換を行ってもよい。

【００１１】上記ＩＫＥフェーズ１（１５０１）では、ＩＫＥ自身が安全に通信を行うために、互いに利用可能なＳＡ(Security Association)を確立するための情報を交換する。ここでＳＡとは、例えば、認証アルゴリズムや認証パラメータ、暗号化アルゴリズムや暗号化パラメータ等を含む一連の定義情報群である。

【００１２】次に、ＩＫＥフェーズ２（１５０２）では、前記ＩＫＥフェーズ１にて確立した上記ＳＡを用いて、ＩＰＳＥＣ通信用のＳＡに関する情報を交換する。ここで、ＩＰＳＥＣ通信用のＳＡの一例について図１８に示す。図１８は、複数の上記ＳＡである、ＳＡ－１（１８０２）～ＳＡ－Ｍ（１８０３）を含むＳＡＤ１８０１であり、さらに各ＳＡにはアドレス情報１８０４、インデックス情報であるＳＰＩ１８０５（Security Parameters Index）、及びセキュリティパラメータであるＳＡＰ１８０６が含まれる。上記アドレス情報１８０４には送信先ＩＰアドレス、送信先ポート番号、送信元ＩＰアドレス、送信元ポート番号、プロトコル番号等が含まれる。又、上記ＳＰＩ１８０５には、擬似乱数等が用いられ、上記ＳＡＰ１８０６は、認証アルゴリズム、暗号化アルゴリズム、暗号化鍵等のセキュリティ通信のレベルに直接関連する情報を持つ。例えば上記ＳＡＰ－１（１８０６）の場合、認証アルゴリズムとしてＨＭＡＣ－ＭＡ５を、暗号化アルゴリズムとしてＤＥＳ－ＣＢＳが含まれる。

【００１３】上記ＩＫＥフェーズ２（１５０２）で行われるＩＰＳＥＣ通信用のＳＡに関する情報の交換は、具体的には、ネットワーク接続装置１４０２がネットワーク接続装置１４０３に対し、ＩＰＳＥＣ通信に使用する上記ＳＡの構成の提案を送信し、該ネットワーク接続装置１４０３は上記提案の中から受け入れ可能なＳＡを返信するものである。ここで、上記ＳＡの構成の提案は、上記ネットワーク接続装置１４０２の後述するデータ記憶部２１０３に予め記憶されている認証アルゴリズム、暗号化アルゴリズム等を用いて構成される。上記ネットワーク接続装置１４０２がどの様な認証アルゴリズム、暗号化アルゴリズムを搭載しているかは、ネットワーク接続装置により異なる。また、予め上記ネットワーク接続装置１４０２が提案するＳＡを決めておくことも可能である。

【００１４】上記ＳＡの返信処理により、ＩＰＳＥＣ通信に使用されるＳＡが確立される。上記確立されたＩＰＳＥＣ通信に使用されるＳＡの情報は、図１８に示すＳＡＤ１８０１及び、図１７に示すＳＰＤ１７０１に格納される。該ＳＰＤ１７０１の構成は以下の例に示される。即ち、送信先ＩＰアドレス１７０２、ＩＰＳＥＣ処理の有無１７０３、上記ＳＡＤ１８０１における各ＳＡの位置を示すアドレスポインタ１７０４、及び上記送信先ＩＰアドレス１７０２にデータを送信する場合に、ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１７０５である。ここで、上記ＩＰアドレス１７０５は、具体的にはネットワーク接続装置１４０３のＩＰアドレスとなる。ここで、送信の通信端末がＩＰＳＥＣ機能を搭載している場合、上記ＩＰアドレス１７０２が上記ＩＰアドレス１７０５と同一となる。また、上記送信先ＩＰアドレス１７０２及び１７０５は範囲指定が可能である。範囲指定とは、具体的にはＩＰアドレスを用いて例えば”１９２．１６８．１．１～１９２．１６８．１．１００”という指定を指し、上記範囲指定により１つの指定で例えば２００台の通信端末へのデータの送信を指定することが出来る。尚、上記ＳＡは片方向で１つ設定されるので、双方通信の場合は独立したＳＡがネットワーク接続装置１４０２、１４０３にそれぞれ設定される。

【００１５】上記ＩＰＳＥＣ通信に使用されるＳＡが確立された後、送信側のコンピュータ１４０１から上記コンピュータ１４０４に送信されるデータは、該コンピュ

ータ１４０１にてＩＰヘッダを付加され、ＩＰパケットとしてＬＡＮ１４０７を介してネットワーク接続装置１４０２に送られる。該ネットワーク接続装置１４０２は、後述するＩＰＳＥＣ処理を行うことにより上記ＩＰパケットをＩＰＳＥＣパケット１５０３として、上記ネットワーク接続装置１４０３に送信する。上記ＩＰＳＥＣパケット１５０３を受信した上記ネットワーク接続装置１４０３は、同じく後述するＩＰＳＥＣ処理にて上記ＩＰＳＥＣパケット１５０３をＩＰパケットに戻し、上記ＬＡＮ１４０８を介して上記コンピュータ１４０４に送信する。即ち、上記インターネット１４０９を介して接続される上記ネットワーク接続装置１４０２、１４０３間では、送信側のコンピュータ１４０１から上記コンピュータ１４０４に送信されるデータはＩＰＳＥＣによりセキュリティが確保される。

【００１６】続いて、図１４、図１６、図１９、図２０を用いて上記ネットワーク接続装置１４０２及び１４０３におけるＩＰＳＥＣ処理の詳細を説明する。ここに図１６は、ＡＨ(Authentication Header) フォーマット及び、ＥＳＰ(Encapsulation Security Payload)ヘッダフォーマットの詳細図、図１９は、送信側ネットワーク接続装置におけるＩＰＳＥＣ処理のフローチャート、図２０は、受信側ネットワーク接続装置におけるＩＰＳＥＣ処理のフローチャートである。

【００１７】尚、後述するＳＰＤ、ＳＡＤはそれぞれのネットワーク接続装置内のデータ記憶部２１０３に記憶されている。ここで、図１９、２０におけるＳはステップを意味する。

【００１８】上記ネットワーク接続装置１４０２では、送信側のコンピュータ１４０１より送信されたＩＰパケットを受信すると、まずその送信先ＩＰアドレスを読み出す（図１９：Ｓ１９０１）。つづいて該送信先ＩＰアドレスを基に上記ネットワーク接続装置１４０２に格納される上記ＳＰＤ１７０１の送信先ＩＰアドレス１７０２を検索し、対応するＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１７０５、ＩＰＳＥＣ処理の有無１７０３及びＳＡの位置を示すアドレスポインタ１７０４を読み出す（図１９：Ｓ１９０２）。

【００１９】ここで、ＩＰＳＥＣ処理を行わない設定、即ちＩＰＳＥＣ処理の有無１７０３が”無”の場合、上記受信したＩＰパケットをそのまま上記ネットワーク接続装置１４０３に送信する（図１９：Ｓ１９０３のＮｏ）。

【００２０】ＩＰＳＥＣ処理を行う設定、即ちＩＰＳＥＣ処理の有無１７０３が”有”の場合、更に上記ＳＡの位置を示すアドレスポインタ１７０４を用いて上記ＳＡＤ１８０１を検索し、該当するＳＡの内容を読み出す（図１９：Ｓ１９０３のＹｅｓ→Ｓ１９０５）。該ＳＡは、上記ＩＫＥフェーズ２（１５０２）で確立されたＳＡである。次に、上記ネットワーク接続装置１４０２は、上記ＳＡの内容に従い、例えば認証アルゴリズムとしてＨＭＡＣ－ＭＡ５を、暗号化アルゴリズムとしてＤＥＳ－ＣＢＳを用いて上記ＩＰパケットから認証／暗号化データを作成する（図１９：Ｓ１９０５）。さらに、上記ネットワーク接続装置１４０２は、上記認証／暗号化データに、認証ヘッダＡＨまたは認証／暗号化ヘッダＥＳＰを追加し、ＩＰＳＥＣ処理を施したＩＰパケット（ＩＰＳＥＣパケット１５０３）とする（図１９：Ｓ１９０６）。ここで、上記ＡＨ及びＥＳＰには上記ＩＫＥフェーズ２で確立したＳＡを構成する上記ＳＰＩ１８０５が含まれる。続いて上記ＩＰＳＥＣパケット１５０３は、インターネット１４０９を介して上記ＳＰＤ１７０１のＩＰアドレス１７０５が示す上記ネットワーク接続装置１４０３に送信される。ここで、ＩＰＳＥＣの処理には”トランスポートモード”と”トンネルモード”があり、上記説明はトンネルモードの説明であるが、例えば上記トランスポートモードを使用する場合には上記ＩＰパケットの送信先ＩＰアドレスは暗号化されない。又、上記トランスポートモード及びトンネルモードは適宜選択可能である。尚、上記ＡＨフォーマット及びＥＳＰヘッダフォーマットの詳細を図１６（ａ）、（ｂ）に示す。

【００２１】次に、上記ネットワーク接続装置１４０３は、受信したＩＰパケットがＩＰＳＥＣパケットであるかを判別する（図２０：Ｓ２００１）。

【００２２】ここで、ＩＰＳＥＣパケットでない場合、上記ＩＰパケットはそのままＬＡＮ１４０８を介してコンピュータ１４０４に送信される（図２０：Ｓ２００１のＮｏ）。

【００２３】受信したＩＰパケットが、ＩＰＳＥＣパケットである場合、以下の処理を行う（図２０：Ｓ２００１のＹｅｓ）。即ち、まず上記ＩＰＳＥＣパケット内の上記ＡＨやＥＳＰヘッダを調べ、該ＡＨやＥＳＰヘッダに含まれるＳＰＩを読み出す（図２０：Ｓ２００２）。次に、上記ネットワーク接続装置１４０３に格納されるＳＡＤを上記ＳＰＩを用いて検索し、上記ＳＰＩに該当する、上記ＩＫＥフェーズ２で確立したＳＡの内容を読み出す（図２０：Ｓ２００３）。これにより、上述したＩＫＥフェーズ２で確立した該当ＳＡが読み出されることになる。ここで、Ｓ２００２にて該当ＳＰＩが無い場合はユーザにその旨を表示して処理を終了する（図示せず）。

【００２４】さらに、上記ネットワーク接続装置１４０３は、上記読み出したＳＡで指定された認証／暗号化アルゴリズム等を用いて、上記ＩＰＳＥＣパケットの認証／暗号化データを認証／復号化する（図２０：Ｓ２００４）。又、必要に応じて上記ＳＡのアドレス情報１８０４からＳＰＤ１７０１を検索し、送信元のＩＰアドレス及び、ＩＰＳＥＣ処理の有無を確認し、元のＩＰパケットを生成する（図２０：Ｓ２００５→２００６）。続い

て上記ネットワーク接続装置１４０３は生成した上記ＩＰパケットをコンピュータ１４０４に送信する。

【００２５】以上により、上記認証／復号化された上記ＩＰＳＥＣパケットの認証／暗号化データは、ＩＰパケットとしてＬＡＮ１４０８を介してコンピュータ１４０４に送信される。即ち、上記ネットワーク接続装置１４０２、１４０３間では、送信側のコンピュータ１４０１から上記コンピュータ１４０４に送信されるデータはＩＰＳＥＣにてセキュリティが確保される。

【００２６】続いて、図２１を用いて上記ネットワーク接続装置１４０２の構成の概略を説明する。尚、ネットワーク接続装置１４０３も同様の構成である。

【００２７】上記ネットワーク接続装置１４０２及び１４０３は、一般的に図２１に示すような構成を有する。即ち、処理部２１０１、一時データ記憶部２１０２、データ記憶部２１０３、システム制御部２１０４、ネットワーク制御部２１０６、回線制御部２１０７が内部バス或いはスイッチ２１０５にてそれぞれ接続されている。また、上記ネットワーク制御部２１０６は上記ＬＡＮ１４０７に、上記回線制御部２１０７はインターネット１４０９とそれぞれ接続されている。

【００２８】上述したＳＰＤ、ＳＡＤは、フラッシュメモリ、ハードディスク、ＲＯＭ等の不揮発性メモリで構成された上記データ記憶部２１０３に格納される。上記処理部２１０１は、上記ネットワーク接続装置１４０２の電源投入時に上記データ記憶部２１０３からシステム制御部２１０４を経由して、上記ＳＰＤ，ＳＡＤを読み出し、ＤＲＡＭ、ＳＲＡＭ等の揮発メモリで構成される上記一時データ記憶部２１０２に格納するかあるいは、必要なときに読み出し、一時データ記憶部２１０２に格納する。又、上記ＳＰＤ、ＳＡＤの更新は上記データ記憶部２１０３に格納されているＳＰＤ、ＳＡＤに対して行なわれる。

【００２９】ＬＡＮ１４０７或いはインターネット１４０９からそれぞれネットワーク制御部２１０６、回線制御部２１０７を経由して受信した個々のＩＰパケット（ＩＰＳＥＣパケット）は、上記処理部２１０１にて上述したＩＰＳＥＣ処理が行われる。即ち、上記処理部２１０１は、個々のＩＰＳＥＣパケットの上記ＡＨ、ＥＳＰ情報を読み出し、上述した処理フローに従って上記一時データ記憶部２１０２に格納された必要なＳＰＤ、ＳＡＤを検索してＩＰＳＥＣに関する認証／暗号化、認証／復号化を行なった後、送信先アドレスに送信する。また、その他の機能（ルーティング機能等）も上記処理部２１０１にて提供される。

【００３０】ここで、個々のＩＰパケット処理時に、一時データ記憶部２１０２に格納されたＳＰＤ、ＳＡＤを検索する理由は、上記一時データ記憶部２１０２がデータ記憶部２１０３に比べて高速にアクセス可能であり、上記ＩＰＳＥＣ処理の高速化を図ることができるためである。

【００３１】このように、一時データ記憶部２１０２に格納されたＳＰＤ、ＳＡＤを参照して処理を進めるため、例えばＳＡに関するパラメータが変更された場合、変更後のＳＡパラメータが上記ＩＰＳＥＣを用いた通信に反映されるのは、一般的に上記ネットワーク接続装置１４０２の電源投入時及び、リセット時等の起動時のみである。これは通常、ルータ等のネットワーク接続装置１４０２は連続通電され、常時運用されており、一時データ記憶部２１０２に格納されたＳＡに関するパラメータと変更されたパラメータとの整合をとる機構が必要なためと、現状のＩＰＳＥＣを用いた通信は、主に例えば本社と支社間等、決まったネットワーク接続装置間でのＬＡＮ間接続に用いられているため、上記データ記憶部２１０３に格納されるＳＰＤ、ＳＡＤ、その他の設定パラメータについて、変更される機会が少ないことを前提にしているためである。

【００３２】

【発明が解決しようとする課題】上記のようなネットワーク層でのセキュリティプロトコルは、通信パケット全体に対してセキュリティを確保するため、アプリケーションごとにセキュリティを施す必要がなく、ＬＡＮ間接続時のセキュリティ対策として利便性が高い。しかしながら、セキュリティに関する認証／暗号化等の処理は非常に計算量が多く、セキュリティの強度（即ち安全性）を高くすれば通信が漏洩する可能性が低くなるが、それだけ各コンピュータやネットワーク接続装置の負荷が高くなり、即ち、処理の遅延を招く。ここで、セキュリティの強度を下げれば当然通信が漏洩する可能性が高くなる。

【００３３】従来技術では、上記のように相手先端末に対応してセキュリティ通信のレベルを設定しているため、例えば複数のユーザが使用する送信元端末から、暗号化の必要ないユーザが送信するデータにも、一定強度のセキュリティを付与する必要があった。このような通信は、各コンピュータやネットワーク接続装置の不必要な負荷を増大させ、即ち処理の遅延を招くに至っている。逆に、レベルの高いセキュリティを必要とするユーザが送信するデータであっても、それより低いレベルのセキュリティでしか送信できない難点があった。

【００３４】また、従来のＩＰＳＥＣ機能を搭載したルータ等では、予め上述したように通信先のＩＰアドレスに対して使用するＳＡを対応付ける必要があり、さらにその対応付け手続きの困難性から、セキュリティ通信のレベルを柔軟に変更できないばかりでなく、専門知識のないユーザが各自で適宜セキュリティ通信のレベルを変えることが困難であった。しかしながらインターネットあるいは企業間のイントラネットを介した電子メールの交換や、これらを利用した電子商取引が一般化しつつあるため、ネットワークに関する専門的な技術を持った保

守者がいる大企業等だけでなく、そのような専門的な技術者が期待できないＳＯＨＯ（Small Office Home Office）や家庭においても使用できるような容易な設定方法が求められる。　また、接続先や、電子商取引時のクレジット番号発信等、通信によって、セキュリティ通信のレベルを最適に変えたい場合があるが、従来の技術では、接続時のセキュリティ通信のレベルが最適かどうか分からないという課題がある。　本発明は、上記課題を解決するために提案するものであり、従来の利便性を損なうことなくデータ送信を行うユーザごとにセキュリティ通信のレベルを設定できると共に、ネットワークに関する専門知識がなくても容易に各種セキュリティ通信のための接続パラメータを変更でき、かつ直ちに該変更の有効性の確認、及び反映を行うことが可能であり、さらに、接続先との通信にどれ程のセキュリティ通信のレベルを設定すれば良いかを自動で決定できるセキュリティ通信方法を提供するものである。

【００３５】

【課題を解決するための手段】本発明は、上記目的を達成するために以下の手段を備える。

【００３６】すなわち、通信端末を使用するユーザの情報とセキュリティ種を対応付けた対応情報を記憶する記憶手段と、上記ユーザの情報に基づいて、上記対応情報からセキュリティ種を決定する上記セキュリティ種選択手段を備える。

【００３７】さらに、上記セキュリティ種選択手段が、上記対応情報の変更時に、上記変更後の情報に基づいた通信の確立を直ちに確認する構成がある。

【００３８】ユーザ毎にセキュリティ種を対応付けることにより、従来の利便性を損なうことなくデータ送信を行うユーザごとにセキュリティ通信のレベルを設定できる。又、上記対応情報の変更時に、上記変更後の情報に基づいた通信の確立を直ちに確認できることで、直ちに該変更の有効性の確認、及び反映を行うことが可能である。

【００３９】又、通信端末にて動作するアプリケーションに入力されるインターネットアドレス情報と、セキュリティ種とを対応付けた対応情報を記憶する記憶手段と、上記インターネットアドレス情報に基づいて、上記対応情報からセキュリティ種を決定する上記セキュリティ種選択手段を備える。

【００４０】さらに、上記通信端末を使用するユーザの情報とセキュリティ種とを対応付けた構成がある。

【００４１】当該手段により、ユーザになじみの深いインターネットアドレス情報をセキュリティ種と対応付けることにより、ネットワークに関する専門知識がなくても容易に各種セキュリティ通信のための接続パラメータを変更できる。

【００４２】又、通信装置が、セキュリティ種を所定のセキュリティ情報装置に問い合わせる問い合わせ手段と、上記問い合わせに対応する回答に基づいて上記セキュリティ種を決定する上記セキュリティ種選択手段を備え、さらに上記セキュリティ情報装置が、通信装置の端末特定情報と、該通信装置との通信において推奨されるセキュリティ種とを対応付けた対応情報を記憶する記憶手段と、他の通信装置からの、上記通信装置について推奨されるセキュリティ種の問い合わせに対し、上記推奨されるセキュリティ種を選択する推奨セキュリティ種管理手段と、上記選択された推奨されるセキュリティ種を送信する送信手段を備える。

【００４３】当該手段により、上記セキュリティ情報装置にセキュリティ種を問い合わせることにより、接続先との通信にどれ程のセキュリティ通信のレベルを設定すれば良いかを自動で決定できる。

【００４４】尚、上記セキュリティ種が、セキュリティプロトコルである場合や、認証アルゴリズムや暗号化アルゴリズムを含む定義情報群である構成がある。

【００４５】また、セキュリティ通信方法は、各通信装置又は通信端末に上述した手段をそれぞれ備えることにより実現する。

【００４６】

【発明の実施の形態】以下、添付図面を参照して、主に従来例との違いについて本発明の実施の形態につき説明し、本発明の理解に供する。尚、以下の実施の形態は、本発明を具体化した一例であって、本発明の技術的範囲を限定する性格のものではない。

【００４７】〔実施の形態１〕始めに、図１、図２（ａ）、図２（ｂ）、図４を参照しながら、実施の形態１におけるセキュリティ通信方法、通信システム及びその装置の概略について説明する。

【００４８】図１は本発明に係るセキュリティ通信方法を用いたシステムの概略を示す図である。当該図１において、コンピュータ１０１はＬＡＮ１０７で他のコンピュータ１０５及びネットワーク接続装置１０２と接続されており、ネットワーク接続装置１０２を経由して、外部のインターネット１０９やイントラネット等のＷＡＮに接続されている。このインターネット１０９には他のネットワーク接続装置１０３、ＬＡＮ１０８が接続されており、該ＬＡＮにはコンピュータ１０４、１０６が接続されている。ここで、上記ネットワーク接続装置１０２、１０３は、ルータ、ゲートウエイ、プロキシサーバ等のファイアウォールやＶＰＮ専用装置等である。さらに、上記コンピュータ１０１、１０５にはそれぞれユーザ認証装置１１０、１１１が接続されている。ここで、コンピュータ１０１他はパーソナルコンピュータ、ワークステーション、サーバ、ノート型パソコン、ＩＰ電話、ＩＰテレビ電話、ＩＰ携帯電話等の通信機能を持つ端末であればよい。以下、従来例と同様に、ネットワーク接続装置１０２、１０３間でＩＰＳＥＣ処理を行うものとして説明を行う。尚、ＩＰＳＥＣ処理を行うのは前

記ネットワーク接続装置１０２、１０３に限定するものではなく、送信元コンピュータ１０１、送信先コンピュータ１０４間でも良く、また、コンピュータ１０２、ネットワーク接続装置１０３間でも良いのは従来例と同様である。又、図２（ａ）は本実施の形態１において用いられるユーザ毎のＳＰＤであり、図２（ｂ）はユーザ毎のＳＡＤの例である。上記ユーザ毎のＳＰＤ及びユーザ毎のＳＡＤ内容の詳細は後述する。

【００４９】まず、図４の上記ネットワーク接続装置１０２（１０３も同様の構成である）の構成の概略図を用いて上記ネットワーク接続装置１０２、１０３の内部の処理を説明する。

【００５０】本実施の形態における上記ネットワーク接続装置では、ユーザ毎に異なるセキュリティレベルを設定することを可能にするため、後述するユーザの設定及び送信先のＩＰアドレスの設定を行なう。このため、従来使用されているネットワーク接続装置のような本社と支社間等の決まったＬＡＮを接続している場合でも、例えばユーザの追加等、設定の更新が従来より多いことが予想される。このような更新の都度従来のような装置電源投入や装置リセット等を行なうと通信が短時間でもストップすることとなり、ユーザにとっては不便である。そこで、上記ネットワーク接続装置の内部処理を以下のようにすることにより、装置電源投入や装置リセット等を行なうことなく常時運用を実現する。

【００５１】即ち、図４において、ネットワーク接続装置１０２、１０３は処理部４０１、一時データ記憶部４０２、データ記憶部４０３、システム制御部４０４、ネットワーク制御部４０６、回線制御部４０７を備え、それぞれ内部バス或いはスイッチ４０５にて接続されている。ここで、上記処理部４０１、一時データ記憶部４０２、システム制御部４０４は後述する処理におけるセキュリティ種選択手段４０８として機能する。

【００５２】さらに、上記ユーザ毎のＳＰＤ２０１及び上記ユーザ毎のＳＡＤ２０７はフラッシュメモリ、ハードディスク、ＲＯＭ等の不揮発メモリで構成されたデータ記憶部４０３に格納されている。また、上記ネットワーク接続装置１０２の電源投入時に上記処理部４０１は、上記データ記憶部４０３からシステム制御部４０４を経由して、上記ユーザ毎のＳＰＤ２０１、ユーザ毎のＳＡＤ２０７を読み出し、ＤＲＡＭ、ＳＲＡＭ等の揮発メモリで構成される上記一時データ記憶部４０２に格納する。以後、上記処理部４０１では、上記一時データ記憶部４０２に格納された上記ユーザ毎のＳＰＤ２０１、ユーザ毎のＳＡＤ２０７を用いてＩＰＳＥＣ処理が行なわれる。又、設定の変更に伴う上記ユーザ毎のＳＰＤ２０１、ユーザ毎のＳＡＤ２０７の更新はデータ記憶部４０３に格納されているユーザ毎のＳＰＤ２０１、ユーザ毎のＳＡＤ２０７に対して行なわれる。ここまでの処理は、上記ユーザ毎のＳＰＤ２０１及び、ユーザ毎のＳＡＤ２０７の構造を除き、前記従来技術と同様である。

【００５３】ここで、従来技術では、一時データ記憶部に格納されたＳＰＤ、ＳＡＤを参照してＩＰＳＥＣ処理を進め、再度データ記憶部からＳＰＤ、ＳＡＤが読みだされるのは装置電源投入や装置リセット等を行なった後の装置起動時のみであった。このため、ＳＰＤ、ＳＡＤが変更された場合、その更新されたＳＡがＩＰＳＥＣ処理に反映されるのは、同じく装置電源投入時及び装置リセット時等の装置起動後であった。

【００５４】しかし、本実施の形態では、上記データ記憶部４０３の上記ＳＰＤ、ＳＡＤが設定の変更等により更新された場合には以下の処理を行なう。即ち、上記処理部４０１は、上記一時データ記憶部４０２に格納されているＳＰＤ、ＳＡＤを用いて通信処理を行なっている場合は該処理中の処理が終わり次第通信を中断するとともに、更新されたＳＰＤ、ＳＡＤをデータ記憶部４０３から読み出し、上記一時データ記憶部４０２に格納された該当するＳＰＤ、ＳＡＤに上書きする。ここで、上書きするのは上記更新されたＳＰＤ、ＳＡＤのみであり、ユーザ毎のＳＰＤのうち、更新されていないものについては更新を行わない。これにより、更新に関係しないＳＰＤ、ＳＡＤを用いて通信を行っているユーザのＩＰＳＥＣ通信には影響を及ぼさない。

【００５５】次に、該格納されたＳＰＤ、ＳＡＤを用いて上述したＩＫＥフェーズ２を用いてＳＡを再確立し、新たに確立された該ＳＡを用いてＩＰＳＥＣ処理を再開する。

【００５６】上述したＳＰＤ、ＳＡＤの更新処理を行なうことにより、セキュリティ通信のレベルを変更した場合でも、装置を再度起動する必要がなく、直ちに更新の有効性の確認、即ちＩＫＥフェーズ２を用いたＳＡの再確立、及び更新の反映を行うことが可能である。

【００５７】尚、ＩＰＳＥＣ通信中のＳＡの再確立については、通信を中断して即時再確立を行なう方法や、処理中のＩＰＳＥＣ通信が終了してから再確立を行う方法を予め選択できるとともに、処理するパケットの種類に応じて上記再確立の方法を選択できるものとする。

【００５８】次に、セキュリティ通信を始めるにあたり予め上記ネットワーク接続装置１０２において、図２に示すユーザ毎のＳＰＤ、ユーザ毎のＳＡＤ等の定義情報群を設定する手順の詳細を説明する。

【００５９】即ち、まず上記ネットワーク接続装置１０２の管理者は、当該ネットワーク接続装置１０２の上記処理部４０１に対し、上記コンピュータ１０１、１０５を使用するユーザ毎に、各送信先ＩＰアドレスと、通信する際のＩＰＳＥＣ処理を行なうか否かの設定を行ない、ユーザ毎のＳＰＤ（ＳＰＤ－１～ＳＰＤ－Ｎ）設定を行う。尚、ユーザを識別する方法については後述する。ここで、上記各送信先ＩＰアドレスが、例えば上記コンピュータ１０４、１０６のＩＰアドレスを指すこと

は、従来例の場合と同様である。又、該設定は上記コンピュータ１０１、１０５等の例えばＷＥＢブラウザ等より行うか又は、直接ネットワーク接続装置１０２にて行うことができる。又、上記各送信先ＩＰアドレスは従来技術と同様範囲指定が可能である。

【００６０】次に、ＩＰＳＥＣ処理を行なう場合には該ＩＰＳＥＣ処理に使用するＳＡの内容である認証アルゴリズムや認証パラメータ、暗号化アルゴリズムや暗号化パラメータ等を含むユーザ毎の一連の定義情報群ＳＡＤ（ＳＡＤ－１～ＳＡＤ－Ｎ）の設定も行なう。上記設定により、図２（ａ）に示すユーザ毎のＳＰＤ２０１が上記ネットワーク接続装置１０２のデータ記憶部４０３に複数登録され、さらに、上記ＳＡの内容である認証アルゴリズムや認証パラメータ、暗号化アルゴリズムや暗号化パラメータ等を含む一連の定義情報群がユーザ毎のＳＡＤ２０７として登録される。上記登録されたＳＡＤ２０７が含むＳＡは後述するＩＫＥフェーズ２にてネットワーク接続装置１０３に提案される。

【００６１】ここで、図２（ａ）に示すユーザ毎のＳＰＤ２０１は、前記従来技術におけるＳＰＤ１７０１と同様、送信先アドレス２０２、ＩＰＳＥＣ処理の有無２０３、ＳＡの位置を示すアドレスポインタ２０４、送信先ＩＰアドレス２０２にデータを送信する場合に、ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス２０６を含むが、さらにユーザ名２０５によって区別されている点で従来技術と異なる。尚、図２（ａ）にはユーザ毎にＳＰＤを設ける例を示したが、１つのＳＰＤ内に個々のユーザを識別する項目を設けることによりユーザ毎のＳＡを指定してもよい。

【００６２】同様に、図２（ｂ）に示すユーザ毎のＳＡＤ２０７は、図１８に示す従来技術におけるＳＡＤ１８０１と同様の構成を有し、１つのＳＡＤに複数のＳＡを含む。例えば、ＳＡＤ－１にはＳＡ－１１からＳＡ－１Ｍ（２１１）を含み、同様に、ＳＡＤ－ＮにはＳＡ－Ｎ１からＳＡ－ＮＭを含む。また、アドレス情報２０９、インデックス情報であるＳＰＩ２１０、セキュリティパラメータであるＳＡＰ２１２を有する。上記アドレス情報２０９には送信先ＩＰアドレス、送信先ポート番号、送信元ＩＰアドレス、送信元ポート番号、プロトコル番号等が含まれる点も、従来技術と同様である。但し、ユーザ名２０８によって区別されている点で従来技術と異なる。尚、図２（ｂ）にはユーザ毎にＳＡＤを設ける例を示したが、１つのＳＡＤ内に個々のユーザを識別する項目を設けることによりユーザ毎のＳＡを管理してもよい。

【００６３】上記設定が終了すると、上記ネットワーク接続装置１０２は、後述するユーザ情報を元に、上記設定の有効性を確認するために、前記従来技術と同様ＩＫＥフェーズ１及びフェーズ２を用いて、上記ネットワーク接続装置１０３と通信を行ない、上記設定された内容に基づいてＩＰＳＥＣ通信が可能であるかを確認するとともに、通信が可能であればＳＡを確立する。尚、前記ＳＡの確立は、上記設定の終了時に必ずしも行う必要はなく、例えばコンピュータ１０１とコンピュータ１０４が上記ネットワーク接続装置１０２及びネットワーク接続装置１０３を介して通信を開始する場合に行ってもよい。

【００６４】また、上記ネットワーク接続装置１０３に対しても、上記ネットワーク接続装置１０２に対して行なった場合と同様、上記コンピュータ１０４、１０６にユーザ認証装置を接続する等して、当該コンピュータ１０４、１０６を使用するユーザ毎に、各送信先ＩＰアドレスに関する設定を行ってもよい。

【００６５】続いて、上記コンピュータ１０１を使用するユーザの識別方法について説明する。

【００６６】上記コンピュータ１０１を使用するユーザは、該コンピュータ１０１の使用時に上記ユーザを特定することができる固有番号を記憶しているＩＣカードを上記ユーザ認証装置１１０に通して入力する。次に、該ユーザ認証装置１１０より上記固有番号に対応するパスワードを入力する。上記ユーザ認証装置１１０にて入力されたＩＣカードの固有番号と上記パスワードが、あらかじめ設定されているものと一致すれば上記ユーザは認証され、上記コンピュータ１０１を使用可能となる。また上記ユーザの認証により得られたユーザ名が上記コンピュータ１０１に記憶される。

【００６７】尚、上記ユーザの認証はＩＣカードである必要は無く、例えば磁気カード、ワンタイムパスワード、指紋、掌形、掌皺、筆跡、虹彩、顔面形状、声紋、ＤＮＡ等で個人を識別する装置でもよく、さらには、上記ユーザ認証装置を設けず、上記コンピュータ１０１へのユーザ名とパスワードの入力によって上記認証を行ってもよい。さらに、上記あらかじめ設定された固有番号及びパスワードの記憶場所は、上記コンピュータ１０１である必要は無く、例えば固有番号及びパスワードを一元管理するコンピュータを別途設け、ユーザの認証時に上記コンピュータ１０１から上記一元管理するコンピュータに問い合わせを行ってもよい。

【００６８】次に、図１、図２、図３を用いて、上記コンピュータ１０１がインターネット１０９を介して接続される上記コンピュータ１０４と通信を行なう場合の処理の詳細を説明する。以下の処理は、上述した図４におけるセキュリティ種選択手段４０８にて実行される。

【００６９】尚、上記ＩＰＳＥＣ通信に使用されるＳＡが確立された後、送信側のコンピュータ１０１から上記コンピュータ１０４に送信されるデータは、上記コンピュータ１０１にてＩＰヘッダを付加され、ＩＰパケットとしてＬＡＮ１０７を介してネットワーク接続装置１０２に送られる点は前記従来技術と同様である。但し、本実施の形態においては、加えて上記ユーザ認証にて得ら

れたユーザ名を上記ＩＰヘッダのオプション部に挿入する処理が行なわれている。上記オプション部は、上記ＩＰヘッダ中でユーザ（設計者）が任意に使用できるデータエリアである。

【００７０】ネットワーク接続装置１０２では、送信側のコンピュータ１０１より送信されたＩＰパケットを受信すると、まず、該ＩＰパケットに含まれるユーザ名及び送信先ＩＰアドレスを読み出す（図３：Ｓ３０１）。つづいて複数のユーザ毎のＳＰＤ２０１より上記ユーザ名に対応するＳＰＤを選択し、さらに該ユーザ名に対応するＳＰＤから、上記送信先ＩＰアドレスをもとに送信先ＩＰアドレス２０２を検索する（図３：Ｓ３０２）。また、対応するＩＰＳＥＣ処理２０３の有無を確認する。

【００７１】ここで、上記ＩＰＳＥＣ処理２０３が”無”、即ちＩＰＳＥＣ処理を行なわない設定の場合、後述するＩＰＳＥＣ処理は行なわずに上記受信したＩＰパケットをそのまま上記ネットワーク接続装置１０３に送信する（図３：Ｓ３０３のＮｏ）。

【００７２】上記ＩＰＳＥＣ処理２０３が”有”、即ちＩＰＳＥＣ処理を行う設定である場合、さらに、対応する上記ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス２０６及びＳＡの位置を示すアドレスポインタ２０４を読み出すと共に、該アドレスポインタ２０４に基づいて該当するＳＡを読み出す（図３：Ｓ３０４）。尚、当該ＳＡは、上記ＩＫＥフェーズ２で確立されたＳＡである点は、従来技術と同様である。

【００７３】次に、上記ネットワーク接続装置１０２は、上記ＳＡの内容に従い、所定の認証アルゴリズム及び暗号化アルゴリズムを用いて上記ＩＰパケットから認証／暗号化データを作成する（図３：Ｓ３０５）。さらに、上記ネットワーク接続装置１０２は、上記認証／暗号化データに、認証ヘッダであるＡＨまたは認証／暗号化ヘッダであるＥＳＰを追加し、次いで、送信先アドレスを上記ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス２０６としてインターネット１０９を介して上記ネットワーク接続装置１０３に送信する（図３：Ｓ３０６）。

【００７４】以降、上記ネットワーク接続装置１０３が、受信したＩＰパケットがＩＰＳＥＣパケットであるかを判別し、元のＩＰパケットを生成するまでの処理は前記従来技術と同様である。

【００７５】以上のように、予めユーザ毎にＳＰＤを設け、さらに、各通信端末におけるユーザ認証の情報を用いてセキュリティ通信の内容を示すＳＡを決定するため、従来の利便性を損なうことなくユーザに応じて最適なセキュリティ通信のレベルを設定することが可能となる。

【００７６】尚、上述した実施の形態１では、ネットワーク接続装置にＩＰＳＥＣ機能を搭載しているが、当然、コンピュータ１０１や１０４等にＩＰＳＥＣ機能を搭載しセキュリティ通信を行っても問題ない。

【００７７】尚、ＳＡが確立した状態で、ユーザ名に対応するＳＰＤを検索した場合で、該当するＳＰＤが無い場合、及び、ＳＰＤに該当ＩＰアドレスが無い場合（図示せず）、ユーザにその旨を表示し、セキュリティ処理を施さずＩＰパケットを送出しても良いし、また、送信を行わないといったことも可能である。また、ユーザに送信するかどうか問い合わせるといった対応を行ってもよい。尚、ＳＰＤでＩＰＳＥＣ処理を行わない設定になっていた場合は、そのままＩＰＳＥＣ処理を行わず送信先ＩＰアドレスにＩＰパケットを送出する。

【００７８】さらに、本実施の形態では、セキュリティ通信のプロトコルをＩＰＳＥＣに限定しているが、ネットワーク接続装置が複数のセキュリティ通信のプロトコルを搭載している場合には、上記ユーザ情報と上記セキュリティ通信のプロトコルを対応付けることにより、ユーザによってセキュリティ通信のプロトコルを使い分けることが可能になる。上記セキュリティ通信のプロトコルを使い分けることにより、更に多種多様なセキュリティ通信を行なうことが出来る。

【００７９】さらに、本実施の形態ではＩＰＳＥＣを用いて各ユーザに対応するＳＰＤを指定しているが、ＩＰＳＥＣ以外のプロトコルを用いる場合についても同様であり、ユーザ認証情報から対応するＳＰＤもしくはＳＰＤに相当するデータベースを参照して、ＳＡもしくはＳＡに相当する情報を指定することにより、認証アルゴリズム、暗号化アルゴリズム等の一連の定義情報群を指定することが出来る。当然、用いるプロトコルの種類によってはＳＰＤを参照せずに直接ＳＡを指定してもよい。

【００８０】また、ユーザ数が多数の場合等にはユーザ毎にＳＰＤを作成せず、各ユーザが所属するグループを作成し、該グループごとにセキュリティ通信のレベルを変更してもよい。この場合には、ユーザ認証時にグループ情報も併せて管理し、該グループ情報を以て上記ＳＰＤを参照する。

【００８１】尚、本実施の形態では、ユーザ認証にて得られたユーザ名をＩＰヘッダのオプション部に挿入することにより、各ＩＰパケットとユーザ名を対応付けているが、例えばユーザ認証時に該認証内容を各コンピュータがネットワーク接続装置に通知し、該ネットワーク接続装置にて各ユーザ名とコンピュータをそれぞれ対応づけるデータベースを持つことにより各ＩＰパケットとユーザ名の対応付けを行ってもよい。

【００８２】〔実施の形態２〕次に、図５、図６を参照しながら、実施の形態２におけるアプリケーション層のアドレス情報をＳＡに対応づける方法について説明する。ここでアプリケーション層とは、ＯＳＩ参照モデルの第７層を指し、主に通信処理が関係するアプリケーションを意味する。ここで、アプリケーション層のインタ

ーネットアドレス情報はホスト名、あるいはホスト名と接続プロトコルを組み合わせたＵＲＬ（Uniform Resource Locator）表記を含むものとする。また、後述するネットワーク接続装置は上記実施の形態１で示した場合と同様、セキュリティ通信のレベルを変更した場合等でも、装置を再度起動しなおすことなく変更を反映できるものである。

【００８３】図５に示すインターネットアドレスを用いたＳＰＤ５０１は、インターネットアドレス５０２、送信先ＩＰアドレス５０３、ＩＰＳＥＣ処理の有無５０４、ＳＡの位置を示すアドレスポインタ５０５、送信先ＩＰアドレス５０３にデータを送信する場合に、ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス５０６を備える。上記インターネットアドレス５０２を備える点を除いては従来技術におけるＳＰＤ１７０１と同様である。また、上記アドレスポインタ５０５の示すＳＡが含まれるＳＡＤの構成も、従来技術のＳＡＤ１８０１と同様である。さらに、上記インターネットアドレス５０２は具体的には例えば"http://abc.def.com"といったＵＲＬや" abc@def.com"といった電子メールアドレス、同様に電子メールの送受信に使用されるＰＯＰサーバ（Post Office Protocol　サーバ）、ＳＭＴＰサーバ（Simple Mail Transfar Protocol　サーバ）等のアドレスが格納される。

【００８４】まず始めに図６を用いて本実施の形態２における、アプリケーション層のアドレス情報をＳＡに対応づける具体的な操作の例を説明する。図６はＩＰＳＥＣ機能を搭載したネットワーク接続装置の設定を行うコンピュータ等の通信端末装置の概略図である。

【００８５】図６において、通信端末装置本体６０８は、制御手段６０９、ディスプレイ６０１、ネットワーク接続装置管理手段６１０、入力手段６１１、指示入力手段６１２を備える。また、後述する各ソフトウェアは上記制御手段６０９又は該上記制御手段６０９を構成する上記ネットワーク接続装置管理手段にて実行される。また、上記通信端末装置本体６０８を使用するユーザに対する情報の表示等は、必要に応じて上記各ソフトウェアの表示機能により上記ディスプレイ６０１に表示される。

【００８６】まず、上記通信端末装置本体６０８の上記制御手段６０９にて、アプリケーション層のアドレス情報となるＵＲＬ６０３を表示するアプリケーションソフトウェアであるＷＥＢ閲覧ソフトウェア６０２等を実行する。

【００８７】さらに、上記ネットワーク接続装置管理手段６１０にて、ネットワーク接続装置管理ソフトウェア６０５を実行する。該ネットワーク接続装置管理ソフトウェア６０５は、パラメータ設定用ウインドウ６０６及び設定ボタン６０７を表示する機能を有し、上記パラメータ設定用ウインドウ６０６には上記ネットワーク接続装置がサポートする複数のＳＡが表示されている。尚、上記複数のＳＡは、認証アルゴリズム、暗号化アルゴリズム等が異なり、この違いによりセキュリティ通信のレベルが異なるものである。又、上記ディスプレイ６０１は上記ネットワーク接続装置に直接接続され、該ネットワーク接続装置が上記制御手段６０９及びネットワーク接続装置管理手段６１０の機能を提供してもよいが、ネットワーク接続装置とネットワークを介して接続されているコンピュータ（例えばコンピュータ１０１）にて上記制御手段６０９及びネットワーク接続装置管理手段６１０の機能を提供してもよい。この場合には、上記操作は上記コンピュータによって行われ、通信によって上記操作の変更が上記ネットワーク接続装置に反映される。

【００８８】上記ネットワーク接続装置の設定を行うユーザは、上記通信端末装置本体６０８にて、ディスプレイ６０１に表示されているアドレス情報である上記ＵＲＬ６０３等を指示入力手段６１２を用いてドラッグし、上記パラメータ設定用ウインドウ６０６に表示されている複数のＳＡの内の希望する任意の一つにドロップする。上記指示入力手段６１２とは、例えばコンピュータにて一般的に使用されるマウス、トラックボール、ジョイスティック、タッチペン、指等のポインタ指示手段であり、該指示入力手段６１２が指し示すディスプレイ６０１上の位置がポインタ６０４として表示される。この操作により上記アプリケーション層のアドレス情報をＳＡに対応づけることができる。続いて上記設定ボタン６０７をクリックすることにより、上記ネットワーク接続装置にて後述する設定処理が行われる。尚、設定ボタン６０７をクリックした場合、ＩＰＳＥＣ通信の途中であっても、当該通信を中断して、直ちに当該設定更新処理を行うか、当該通信が終了してから直ちに当該設定更新処理を行うかは設定等で選択できるものとする。また、通信を行う場合に初めて当該設定変更があった通信先とセキュリティ通信のための接続を行うか、直ちに前記接続を行うかについても設定等で選択が可能であるものとする。

【００８９】次に、図４、図５、図７を用いて、上記ユーザによる操作が終了した後の上記ネットワーク接続装置にて行われる設定処理を説明する。まず、ネットワーク接続装置の設定を行うユーザが上述したように上記アプリケーション層のアドレス情報をＳＡに対応づけた後、上記ネットワーク接続装置の処理部４０１はデータ記憶部４０３に格納されるＳＰＤ５０１のインターネットアドレス５０２にアプリケーション層のアドレス情報を格納する（図７：Ｓ７０１～Ｓ７０２）。

【００９０】次に上記処理部４０１はＤＮＳサーバ（Domain Name System　サーバ）を用いて上記アドレス情報をＩＰアドレスに変換する（図７：Ｓ７０３）。ここに、ＤＮＳサーバとは、インターネット接続環境があれば一般的に使用できるサービスで、上記アドレス情報で

ある例えば"abc.def.com" といった文字列を用いて問い合わせることにより、上記"abc.def.com" に対応するＩＰアドレスを回答するサーバである。次に、上記処理部４０１は、上記変換したＩＰアドレスを上記ＳＰＤ５０１の送信先ＩＰアドレス５０３に格納し、さらに上記データ記憶部４０３に格納されるＳＡＤ１８０１を構成するアドレス情報１８０４に必要な、送信先ＩＰアドレス、送信先ポート番号、送信元ＩＰアドレス、送信元ポート番号、プロトコル番号等をそれぞれ上記ＳＡＤに格納する（図７：Ｓ７０４）。ここで、上記送信先、送信元ポート番号及びプロトコル番号は、例えば上記アドレス情報の一部である" http" により判断される。

【００９１】上記ＳＰＤ５０１及びＳＡＤ１８０１に必要な情報がそろった後、上記ネットワーク接続装置のセキュリティ選択手段４０８は、上記設定による接続の確認を行うかをユーザに問い合わせる（図７：Ｓ７０５）。尚、ユーザへの問い合わせは、別途設定で自動的に行うかどうかを設定してもよく、また、接続の確認を行う設定アイコン又はボタンを設けて、その設定アイコンまたはボタンが押されたら接続の確認を行うようにしてもよい。

【００９２】接続の確認を行う場合は、上記送信先ＩＰアドレスに対して従来技術同様ＩＫＥフェーズ１、フェーズ２及び、新たに設定された上記ＳＰＤ５０１及びＳＡＤ１８０１の情報を用いて接続確認を行い、該結果をユーザに通知する（図７：Ｓ７０５のＹｅｓ→Ｓ７０７）。以上の処理により、アプリケーション層のアドレス情報のＳＡへの対応付けが完了する。設定後は、上記新たに設定されたＳＰＤ５０１及びＳＡＤ１８０１を用いてセキュリティ通信が行われる。

【００９３】尚、上記接続確認は、特にユーザに問い合わせる必要はなく、自動で確認を行うようにしてもよい。又、後述するセキュリティ情報装置を導入することで上記ＩＰＳＥＣ機能を搭載した通信端末のＩＰアドレスの入力を自動で行うことも可能となる。

【００９４】このように、普段よく使用するアプリケーションで指定するアドレス情報を用いてＳＡの設定を行うことにより、専門知識のないユーザでもＳＡの指定を容易に行うことが出来る。

【００９５】さらに、上記パラメータ設定用ウインドウ６０６のＳＡの表示を、例えば" セキュリティ高" 、" セキュリティ中" 、" セキュリテイ低" 、" セキュリティ無し" といった表示にすることにより、ユーザによるアドレス情報のＳＡへの対応付けをより分かりやすくすることが出来る。

【００９６】尚、本実施の形態２ではＩＰＳＥＣを用いた場合のアドレス情報のＳＡへの対応付け例を示しているが、ＩＰＳＥＣ以外のプロトコルを用いる場合についても同様である。

【００９７】当然、上記実施の形態１にて実施されるユーザ毎のセキュリティ通信と同時に実施しても何ら問題ない。この場合のＳＰＤの例を図８のＳＰＤ８０１に示す。

【００９８】〔実施の形態３〕次に、図９、図１０、図１１、図１２、図１３を参照しながら、実施の形態３におけるセキュリティ情報装置の機能について説明する。図９に示す各種機器等１０１～１１１は図１に示したものと同様であるが、さらにネットワーク接続装置９０２を介してセキュリティ情報装置９０１がインターネット１０９に接続されている。ここで、上記ネットワーク接続装置９０２は特にＩＰＳＥＣ機能を搭載している必要はなく、上記セキュリティ情報装置９０１に対する外部からの不正なアクセスを防ぐものであればよい。

【００９９】上記セキュリティ情報装置９０１は、図１３（ａ）に示される構成を有する。即ち、推奨ＳＡ管理手段１３０１、記憶手段１３０２を具備し、上記推奨ＳＡ管理手段１３０１は、送受信手段１３０４を介して上記ネットワーク接続装置９０２と接続されている。また、図１１に示す推奨するＳＡを検索するための第１のデータベース１１０１及び、図１２に示す推奨するＳＡを検索するための第２のデータベース１２０１が、上記記憶手段１３０２に格納されており、必要に応じて上記推奨ＳＡ管理手段が読み出し可能である。

【０１００】また、ネットワーク接続装置１０２、１０３は、図１３（ｂ）に示すように送受信手段１３０８、記憶手段１３０９、制御手段１３０５を備え、該制御手段１３０５はさらに問い合わせ手段１３０６及び問い合わせ回答手段１３０７を備える。

【０１０１】次に、コンピュータ１０４は、図１３（ｃ）に示すように送受信手段１３１２問い合わせ回答手段１３１１を備える。尚、各手段の機能は適宜説明する。

【０１０２】上記第１のデータベースは、送信先ＩＰアドレス１１０２、ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０３、ＩＰＳＥＣ処理の有無１１０４、ＳＡの位置を表すアドレスポインタ１１０５より構成される。ここで、上記送信先ＩＰアドレス１１０２及びＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０３は、ＩＰアドレスの範囲を登録することも可能である。また、上記ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０３は、ＩＰアドレス１１０２に対してＩＰＳＥＣ処理を行う、ＩＰＳＥＣ機能を搭載した通信端末のＩＰアドレスである。

【０１０３】更に図１２は、推奨するＳＡを格納する第２のデータベース１２０１であり、複数の推奨ＳＡが格納されている。該推奨ＳＡとは、送信先であるＩＰＳＥＣ機能を搭載した通信端末が推奨するＳＡや、第３者機関が規定したＳＡであり、送信先の提供するサービスによってセキュリティ通信のレベルが異なる。尚、図１０

は、理解に供するため、図９から説明に不必要な機器を省略したものである。本実施の形態３では、まず、図９において、ネットワーク接続装置１０２が、ＩＰＳＥＣ通信を行おうとするネットワーク接続装置１０３との間でＳＡの確立を行う前に、セキュリティ情報装置９０１に上記ＩＰＳＥＣ通信にふさわしい推奨ＳＡを問い合わせる。上記ネットワーク接続装置１０２とネットワーク接続装置１０３との間でＳＡの確立を行うのは、例えば上記ネットワーク接続装置１０２及びネットワーク接続装置１０３の初期設定時や、コンピュータ１０１とコンピュータ１０４が上記ネットワーク接続装置１０２及びネットワーク接続装置１０３を介して通信を開始する場合等である。尚、推奨ＳＡでＳＡの確立を図ったにもかかわらず、希望する推奨ＳＡでＳＡが確立できない場合、送信を中止する、あるいはユーザに問い合わせる、そのまま推奨ＳＡ以外のＳＡでＳＡ確立を行い、ＩＰＳＥＣ通信を行う等の方法が考えられる。

【０１０４】ここでコンピュータ１０１とコンピュータ１０４が上記ネットワーク接続装置１０２及びネットワーク接続装置１０３を介して通信を開始する場合の上記推奨ＳＡの問い合わせを想定すると以下のようになる。

【０１０５】即ち、ネットワーク接続装置１０２が上記コンピュータ１０１より上記コンピュータ１０４に送信するＩＰパケットを上記送受信手段１３０８を介して受信すると、上記制御手段１３０５は上記ネットワーク接続装置１０２の上記記憶手段１３０９に格納されるＳＰＤを読み出す。

【０１０６】ここで該ＳＰＤに上記コンピュータ１０４の情報がない場合、上記ネットワーク接続装置１０２は、上記問い合わせ手段１３０６により、セキュリティ情報装置９０１に上記ＩＰＳＥＣ通信にふさわしい推奨ＳＡを問い合わせる（図１０Ｓ１００１）。尚、上記セキュリティ情報装置９０１のアドレスは予め上記ネットワーク接続装置１０２の記憶手段１３０９に格納されているものとする。

【０１０７】上記推奨ＳＡの問い合わせにあたり、上記ネットワーク接続装置１０２は、送信先のコンピュータ１０４のＩＰアドレスを上記セキュリティ情報装置９０１に送信する。上記送受信手段１３０４を介して上記コンピュータ１０４のＩＰアドレスを受信した上記セキュリティ情報装置９０１の推奨ＳＡ管理手段１３０１は、上記コンピュータ１０４のＩＰアドレスを基に、上記記憶手段１３０２に格納されている上記第１のデータベース１１０１の送信先ＩＰアドレス１１０２を検索し、対応する上記ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０３、ＩＰＳＥＣ処理の有無１１０４及び、ＳＡの位置を表すアドレスポインタ１１０５を得る。

【０１０８】さらに、上記推奨ＳＡ管理手段１３０１は、上記アドレスポインタ１１０５を用いて上記記憶手段１３０２に格納されている第２のデータベース１２０１より推奨ＳＡを得、該推奨するＳＡを、上記送受信手段１３０４を介してＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０３、ＩＰＳＥＣ処理の有無１１０４と共に上記ネットワーク接続装置１０２に返送する（図１０Ｓ１００２）。

【０１０９】ここで、上記ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０３には、予め登録された上記ネットワーク接続装置１０３のＩＰアドレスが記憶されている。尚、返送する推奨ＳＡの数は複数であっても構わない。

【０１１０】次に、上記推奨ＳＡ、上記ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０３及びＩＰＳＥＣ処理の有無１１０４を受信したネットワーク接続装置１０２の上記制御手段１３０５は、上記受信したＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０３に基づいてネットワーク接続装置１０３との間で、従来技術で説明したＳＡの確立を行い、ＩＫＥフェーズ２におけるＳＡの候補として、推奨ＳＡを提案する（図１０Ｓ１００３）。

【０１１１】ネットワーク接続装置１０３は受け取った推奨ＳＡでのＩＰＳＥＣ通信が可能な場合は、ネットワーク接続装置１０２に該推奨ＳＡを返送し、ＳＡの確立が行われる（図１０Ｓ１００４）。

【０１１２】従って、上記ネットワーク接続装置１０２がセキュリティ情報装置９０１に推奨ＳＡを問い合わせることによって、相手先と安全に通信が可能なＳＡを知ることができ、該推奨ＳＡによるＩＰＳＥＣ通信が可能となる。

【０１１３】ここで、上記ネットワーク通信装置１０２が上記ＩＰＳＥＣ通信にふさわしい推奨ＳＡの問い合わせを行った場合で、上記セキュリティ情報装置９０１の上記第１のデータベース中に該当ＩＰアドレスの登録がない場合が考えられる（図１０Ｓ１００１）。

【０１１４】このような場合、上記セキュリティ情報装置９０１の上記推奨ＳＡ管理手段１３０１は、該当するコンピュータ１０４に、セキュリティ通信に必要なＳＡの候補を問い合わせる（図１０Ｓ１００５）。

【０１１５】問い合わせを受けた上記コンピュータ１０４は、問い合わせ回答手段１３１１により、該コンピュータ１０４に予め登録されている、ＩＰＳＥＣ機能を搭載したネットワーク接続装置１０３のＩＰアドレスを上記セキュリティ情報装置９０１に返送する（図１０Ｓ１００６）。

【０１１６】上記ＩＰＳＥＣ機能を搭載したネットワーク接続装置１０３のＩＰアドレスを受信した上記セキュリティ情報装置９０１の推奨ＳＡ管理手段１３０１は、上記ネットワーク接続装置１０３に対しＳＡの候補を問い合わせる（図１０Ｓ１００７）。問い合わせを受けた上記ネットワーク接続装置１０３の制御手段１３０５

は、該ネットワーク接続装置１０３の記憶手段１３０９に格納されているＳＡの候補を、問い合わせ回答手段１３０７により上記認証サーバ９０１に送信する（図１０Ｓ１００８）。

【０１１７】上記ＳＡの候補を受信したセキュリティ情報装置９０１の推奨ＳＡ管理手段１３０１は、上記第２のデータベース１２０１に上記候補のＳＡを登録するとともに、上記第１のデータベース１１０１に上記ネットワーク通信装置１０２より問い合わせに使用されたＩＰアドレスと上記候補のＳＡの位置を表すアドレスポインタ１１０５、ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０３、ＩＰＳＥＣ処理の有無１１０４を登録する。さらに、上記推奨するＳＡを、上記送受信手段１３０４を介してＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０３、ＩＰＳＥＣ処理の有無１１０４と共に上記ネットワーク接続装置１０２に返送する（図１０Ｓ１００２）。

【０１１８】但し、問い合わせを受けた上記コンピュータ１０４に上記ネットワーク接続装置１０３のＩＰアドレスが登録されていない場合、やＩＰＳＥＣ機能を搭載した通信端末等が無い場合、或いは上記問い合わせ回答手段１３１１を備えない場合、その旨を上記セキュリティ情報装置９０１に返答するか若しくは返答を行わない。該返答を受けた若しくは返答を受けることが出来なかった上記セキュリティ情報装置９０１は、上記旨を上記ネットワーク接続装置１０２に通知すると共に、上記第１のデータベース１１０１の送信先ＩＰアドレス１１０２に上記コンピュータ１０４のＩＰアドレスを登録し、さらにＩＰＳＥＣ処理の有無１１０４を”無し”とする。このような場合には、上記ネットワーク接続装置１０２の制御手段１３０５は、上記コンピュータ１０１のユーザにセキュリティ通信を行えない旨を通知し、又は通信を行わないといった対応を行ってもよい。

【０１１９】尚、前記従来技術で述べたように、ＩＫＥフェーズ２では、双方通信の場合は独立した２つのＳＡが設定される。よって、ネットワーク接続装置１０２の要請によりＩＫＥフェーズ２によるＳＡの確立を行う際に、上記ネットワーク接続装置１０３の制御手段１３０５は、上記セキュリティ情報装置９０１に対して上記ネットワーク接続装置１０２の推奨ＳＡの問い合わせを行ってもよい（図１０Ｓ１００９）。

【０１２０】上記セキュリティ情報装置９０１の上記第１のデータベース１１０１に上記ネットワーク接続装置１０２の推奨ＳＡが登録されていない場合、上記セキュリティ情報装置９０１の推奨ＳＡ管理手段１３０１が、上記ネットワーク接続装置１０２にＳＡの候補を問い合わせるといった処理が行われる（図１０Ｓ１０１０～Ｓ１０１１）。つづいて、上記問い合わせに対応する回答が上記ネットワーク接続装置１０３に通知される（図１０Ｓ１０１２）。この手順は上記処理Ｓ１００１～Ｓ１００２、Ｓ１００７～Ｓ１００８と同様であるため詳細は省略する。

【０１２１】この様に、セキュリティ情報装置を設けることにより、ユーザが通信先のセキュリティ通信のレベルを考える必要がなく、適切なＳＡを設定可能となる。さらに、例えば上記セキュリティ情報装置を第３者機関が管理することにより、通信先アドレスによって、通信先が提供するサービス内容によってセキュリティ通信のレベルを最適にすることが可能となる。また、セキュリティ情報装置が、自動的に該当する通信端末にＳＡの候補を問い合わせて、該問い合わせの内容を収集することにより推奨ＳＡを一元管理することが可能となり、各ＩＰＳＥＣ機能を搭載した通信端末は、上記セキュリティ情報装置に問い合わせを行うのみで推奨ＳＡの候補を得ることが可能となる。この様なシステムは、例えば複数の会社をＩＰＳＥＣ機能を搭載したルータ等で接続する場合等、ＩＰＳＥＣ通信を適用する規模が大きい場合には特に通信端末に対する設定が簡単に行え、管理者及びユーザの負担軽減等に有効である。

【０１２２】尚、上記セキュリティ情報装置が格納するデータベースを２つに分けているが、特に分ける必要はなく、上記機能が実現できれば１つのデータベースにしてもよい。さらに、上述した項目に限らず、その他ＳＡに必要な情報を格納することができる。

【０１２３】更にセキュリティ情報装置がＲＡＤＩＵＳ（Remote Authentication Dial-InUser Service）サーバを兼ねてもよく、ＩＫＥで交換される鍵情報の管理や、ＳＡと対応するＳＰＩ情報の管理を同時に行い、これら情報を提供してもよい。

【０１２４】また、各コンピュータがＩＰＳＥＣ機能を搭載する場合も上記ネットワーク接続装置と同様、セキュリティ情報装置に問い合わせを行うことができる。

【０１２５】又、上記送信先ＩＰアドレスやＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレスは、ＩＰアドレスを用いているが、特にＩＰアドレスに限定するものではなく、送信先通信端末（コンピュータ）を特定する端末特定情報であれば良く、例えばコンピュータ名やＭＡＣアドレス（Media Access Control Address）、電話番号等でもよい。

【０１２６】さらに、実施の形態３は、上記実施の形態１と組み合わせて使用することが可能であり、この場合には上記制御手段１３０５及び記憶手段１３０９がセキュリティ種選択手段４０８となり、送受信制御部１３０８が、ネットワーク制御部４０６及び回線制御部４０７となる。

【図面の簡単な説明】

【図１】本発明に係るセキュリティ通信方法を用いたシステムの概略を示す図。

【図２】実施の形態１におけるユーザ毎のＳＰＤ及びユーザ毎のＳＡＤの例。

【図３】実施の形態１におけるネットワーク処理装置のＩＰＳＥＣ処理のフローチャート。

【図４】実施の形態１におけるネットワーク接続装置の構成の概略図。

【図５】実施の形態２におけるインターネットアドレスを用いたＳＰＤの例。

【図６】実施の形態２におけるＩＰＳＥＣ機能を搭載したネットワーク接続装置の設定を行うコンピュータ等の通信端末装置の概略図。

【図７】実施の形態２におけるネットワーク接続装置の設定確認処理のフローチャート。

【図８】実施の形態２におけるユーザ毎のインターネットアドレスを用いたＳＰＤの例。

【図９】実施の形態３におけるセキュリティ情報装置を用いたシステムの概略を示す図。

【図１０】セキュリティ情報装置を用いたシステムの処理を説明するための簡易図。

【図１１】セキュリティ情報装置における第１のデータベースの例。

【図１２】セキュリティ情報装置における第２のデータベースの例。

【図１３】実施の形態３における各装置の概略を示すロック図。

【図１４】ＩＰＳＥＣ機能を搭載したルータを使用して

ＶＰＮネットワークを構成したネットワークシステムの概略図。

【図１５】ＩＰＳＥＣ機能を搭載したネットワーク接続装置間でのセキュリティ通信の接続手順を表した図。

【図１６】ＡＨフォーマット、ＥＳＰヘッダフォーマットの詳細図。

【図１７】従来技術におけるＩＰＳＥＣの処理方針を決めるデータベースであるＳＰＤ（Security Policy Database）の例。

【図１８】従来技術におけるＳＡデータベースであるＳＡＤ（Security Association Database)の例。

【図１９】従来技術における送信側ネットワーク接続装置のＩＰＳＥＣ処理のフローチャート。

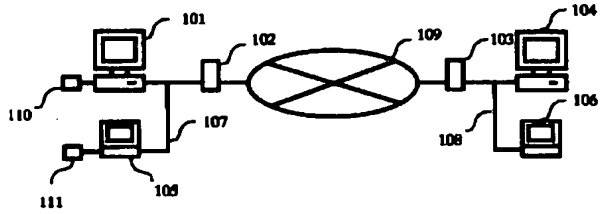
【図２０】従来技術における受信側ネットワーク接続装置のＩＰＳＥＣ処理のフローチャート。

【図２１】従来技術におけるネットワーク接続装置の構成の概略。

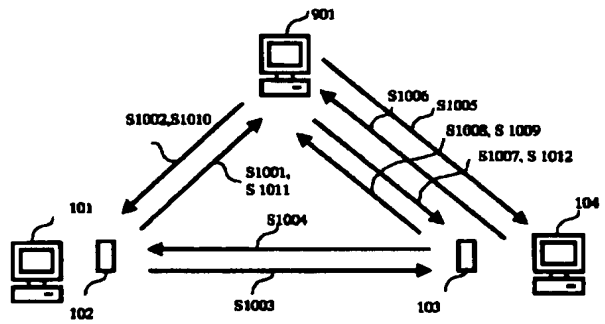
【符号の説明】

１０１、１０４、１０５、１０６	コンピュータ
１０２、１０３	ネットワーク接続装置
１０９	インターネット
１１０、１１１	ユーザ認証装置

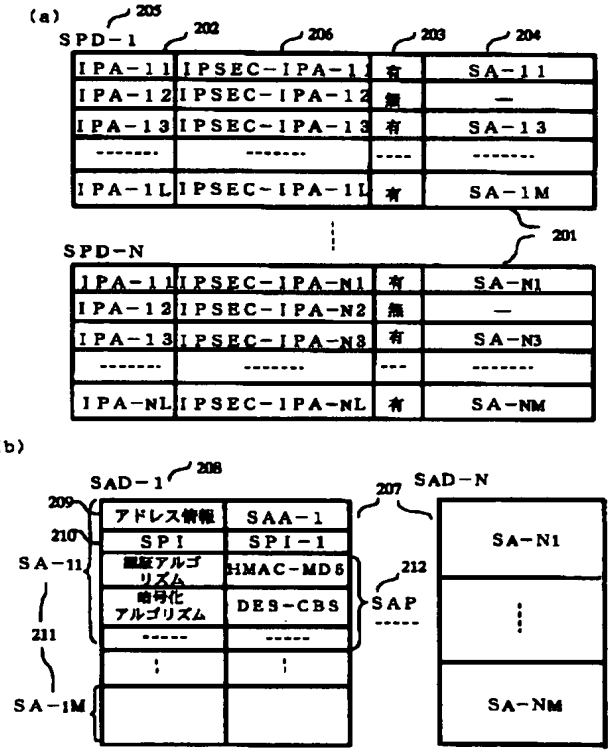
【図１】



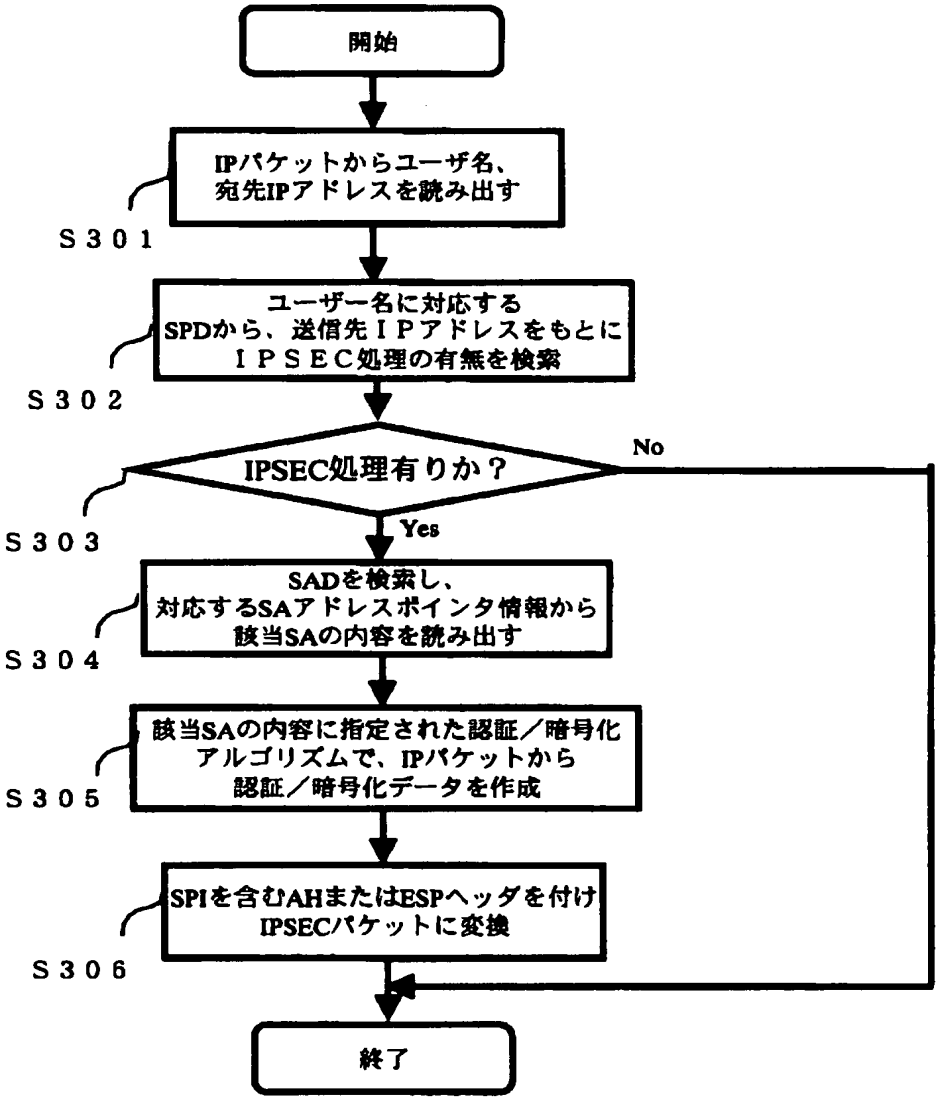
【図１０】



【図２】



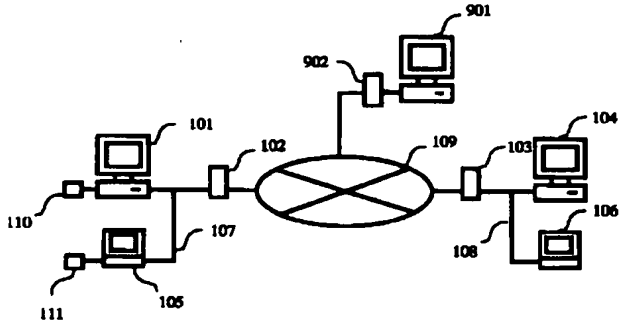
【図３】



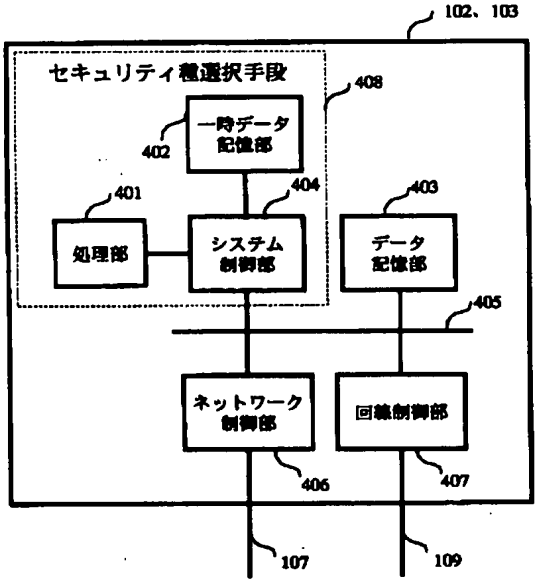
【図５】

501	502	503	506	504	505
APA−1	IPA−1	IPSEC−IPA−1	有	SA−1
APA−2	IPA−2	IPSEC−IPA−2	無	—
-------	IPA−3	IPSEC−IPA−3	有	SA−3
-------	-------	-------	-----	-------
APA−L	IPA−L	IPSEC−IPA−L	有	SA−M

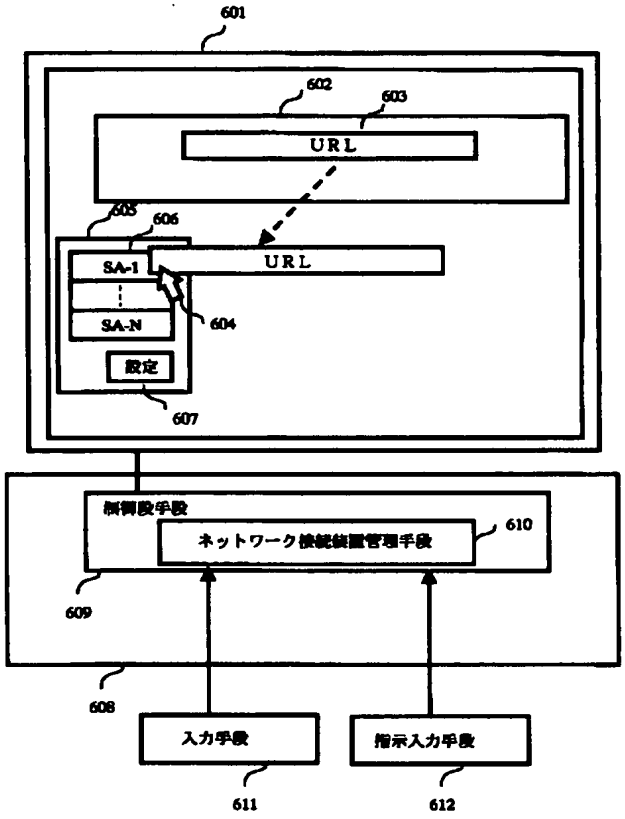
【図９】



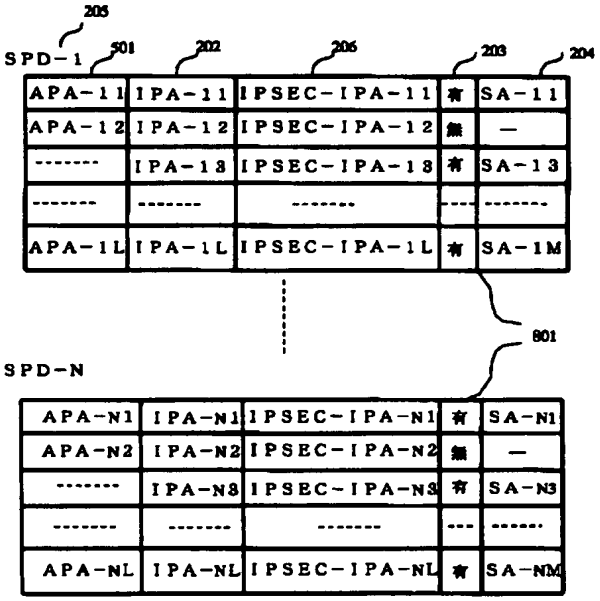
【図４】



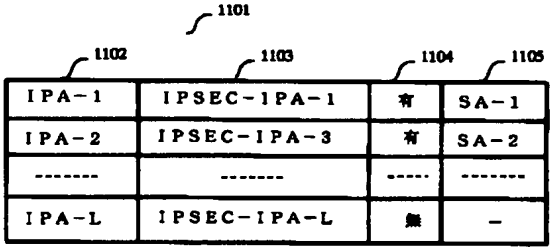
【図６】



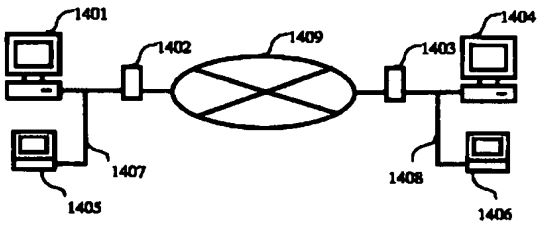
【図８】



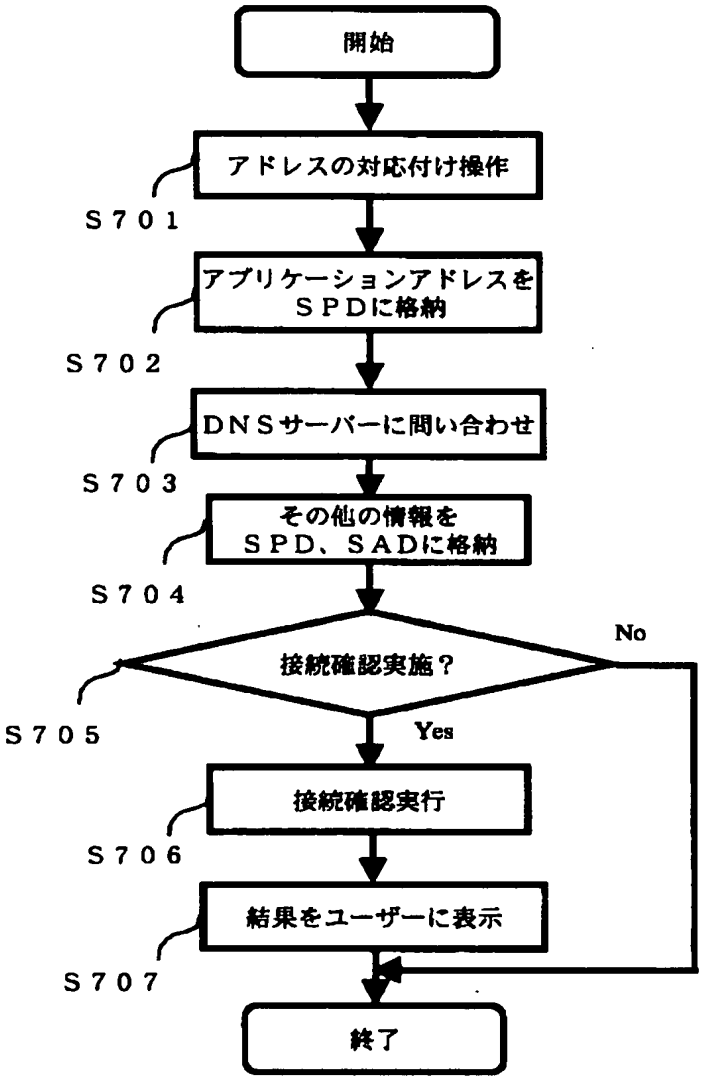
【図１１】



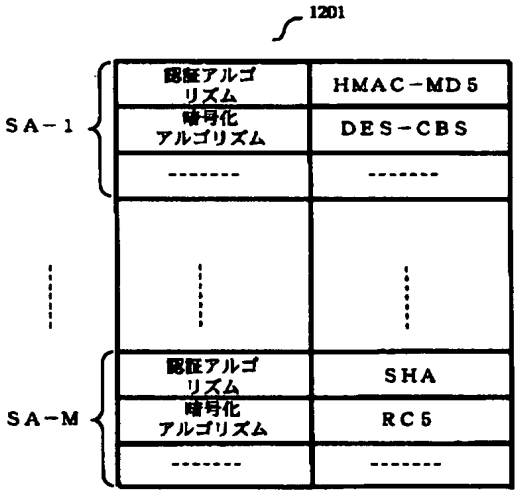
【図１４】



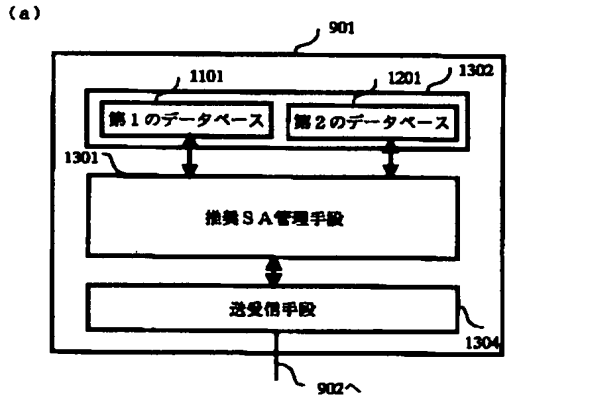
【図７】



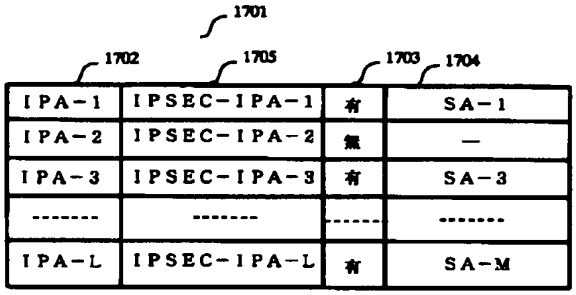
【図１２】



【図１３】



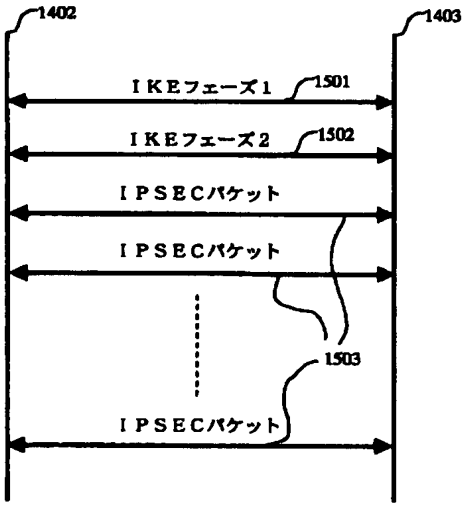
【図１７】



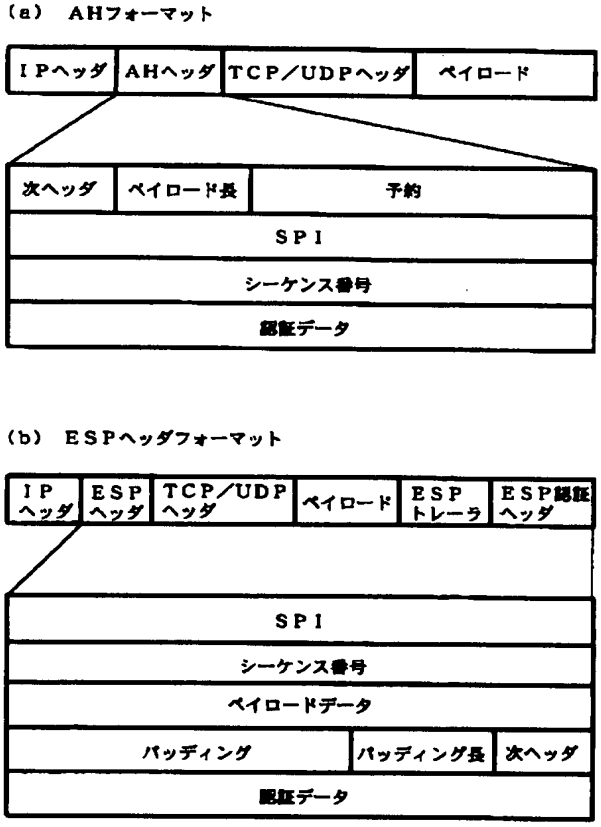
1701

1702	1705	1703	1704
IPA－1	IPSEC－IPA－1	有	SA－1
IPA－2	IPSEC－IPA－2	無	—
IPA－3	IPSEC－IPA－3	有	SA－3
-------	-------	------	-------
IPA－L	IPSEC－IPA－L	有	SA－M

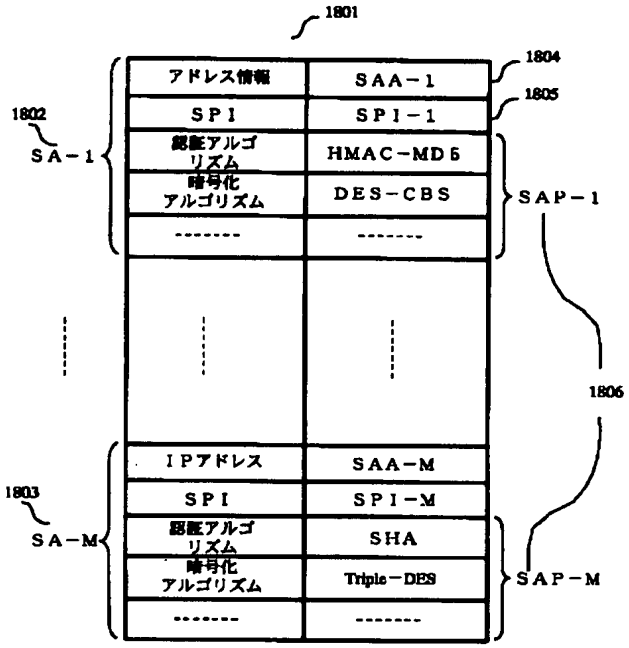
【図１５】



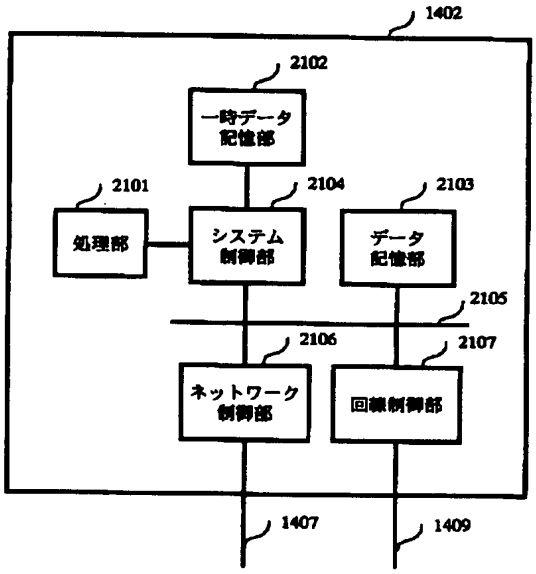
【図１６】



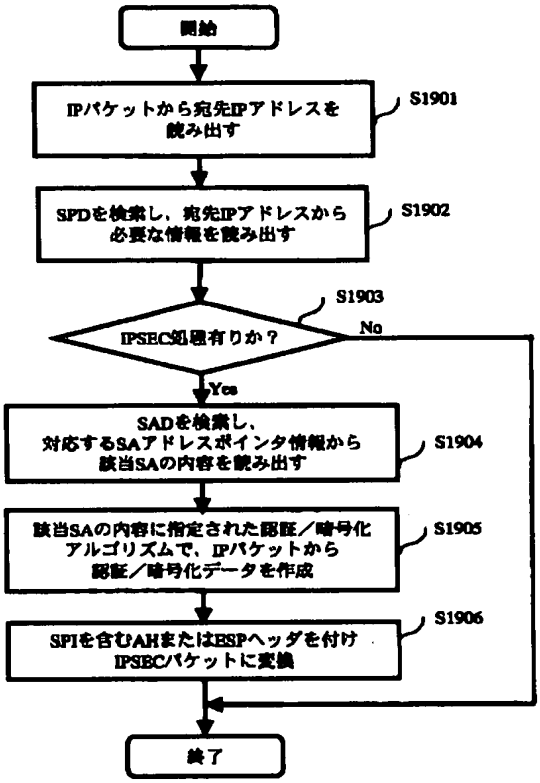
【図１８】



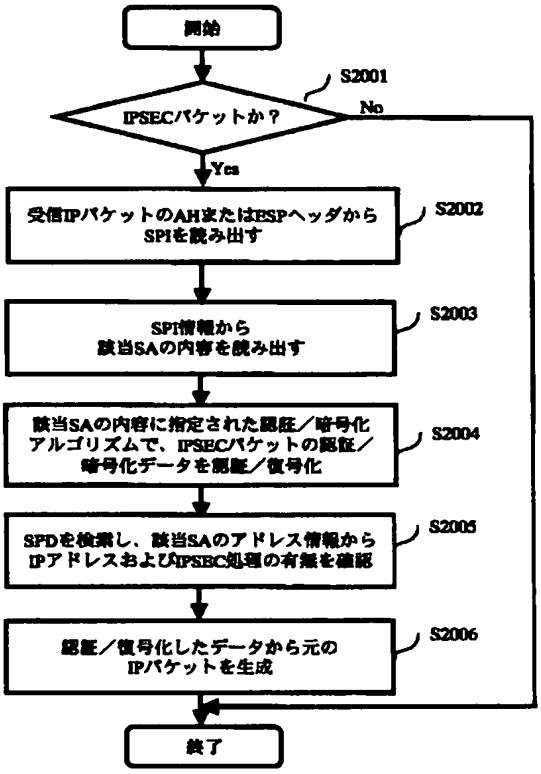
【図２１】



【図１９】



【図２０】



フロントページの続き

(72)発明者　山内　弘貴
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　太田　雄策
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5B085 AE04 AE29
5J104 AA07 AA37 DA03 KA01 PA07